SPECTRUM®

Management Module Guide
for
Standard RMON

CABLETRON SYSTEMS

The Complete Networking Solution™

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Copyright © April 1998, by Cabletron Systems, Inc. All rights reserved.

Printed in the United States of America.

Order Number: 9031280 E4

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

SPECTRUM, the **SPECTRUM IMT/VNM** logo, **DCM**, **IMT**, and **VNM** are registered trademarks, and **SpectroGRAPH**, **SpectroSERVER**, **Inductive Modeling Technology**, **Device Communications Manager**, and **Virtual Network Machine** are trademarks of Cabletron Systems, Inc.

C++ is a trademark of American Telephone and Telegraph, Inc.
UNIX is a trademark of The Open Group.
OSF/Motif and **Motif** are trademarks of the Open Software Foundation, Inc.
X Window System is a trademark of The Open Group.
Ethernet is a trademark of Xerox Corporation.

Virus Disclaimer

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

   Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03866-5005.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.

   (b) This computer software may be:

   (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;

   (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;

   (3) Reproduced for safekeeping (archives) or backup purposes;

   (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;

   (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and

   (6) Used or copied for use in or transferred to a replacement computer.

   (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

   (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.

   (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

Contents

Preface

Who Should Read This Manual xi
How This Manual Is Organized xi

Related Reading xii
Questions about SPECTRUM Documentation xii

Chapter 1 Introduction

RMON Management Module 1-1
SPMA and RMON 1-1
SPECTRUM and RMON 1-2
RMON Models 1-2
Major Software Application Models 1-4
    Minor Software Application Models 1-4
    Device Models 1-4
RMON Groups 1-5
    Supported RMON Groups 1-5
    Unsupported RMON Groups 1-6

Chapter 2 Modeling RMON in SPECTRUM

How to Model RMON 2-1
Creating a Device Model That Supports RMON 2-1
Enabling RMON for a Cabletron Device 2-3
Configuring RMON as a Network Monitor Point 2-5
    Associating an RMON Probe Model with a Network Interface 2-6
    Copying RMON Probes into Network Models 2-8
    Verifying the Monitor Point 2-9

Chapter 3 Loading and Unloading Profiles

What is a Profile 3-1
Checking Your Agent Configuration 3-2
Creating Custom Profiles 3-3
Loading Profiles 3-4
    Problems When Loading Profiles 3-5
Unloading Profiles 3-6

Chapter 4 Icons and Icon Components

The RMONApp Icon 4-1
RMONApp Icon Subviews 4-2
The RMON Ethernet Probe Icon 4-4
RMONEProbe Icon Subviews 4-5
The RMON Token Ring Probe Icon 4-6
RMONTProbe Icon Subviews 4-7

Chapter 5 Using RMON Views

Views Unique to RMON 5-1
Customizing the RMON Tables 5-3
Loading and Unloading Profiles 5-3
Accessing Ethernet Views 5-3
Ethernet Statistics 5-4
Viewing Performance Statistics on the Segment 5-5
Viewing Network Activity with the Multi-Attribute Line Graph 5-5
Viewing Statistics with the Details Button 5-6
Ethernet History 5-7
Viewing the History Table 5-8
Hosts Control 5-8
Viewing the Host Table 5-10
Viewing the Host Table Detail 5-10
Matrix Control 5-11
Viewing the Matrix Table 5-12
HostTopN Control 5-13
Viewing or Configuring the Top Hosts 5-14
Accessing Token Ring Views 5-15
Mac-Layer Statistics 5-15
Viewing Performance Statistics on the Segment 5-16
Viewing Network Activity With the Multi-Attribute Line Graph 5-16
Viewing Statistics with the Details Button 5-16
Promiscuous Statistics 5-17
Viewing Performance Statistics on the Segment 5-18
Viewing Network Activity With the Multi-Attribute Line Graph 5-18
Viewing Statistics with the Frame Details Button 5-18
Mac-Layer History 5-19
Viewing the History Table 5-20
Promiscuous History 5-20
Viewing the History Table 5-21
Ring Station 5-22
Viewing the Station Order 5-23
Viewing Non-Isolating Errors 5-24
Viewing Isolating Errors 5-24
Other RMON Views 5-25
Accessing RMON Alarms/Events 5-25

Chapter 6 Configuring RMON Alarms and Events

RMON Alarms 6-1
Creating an Alarm 6-2
Modifying and Enabling an Alarm Under Creation 6-5
Modifying a Valid Alarm 6-6
Removing an Alarm 6-7
RMON Events 6-7
Creating an Event 6-7
Modifying and Enabling an Event Under Creation 6-10
Modifying a Valid Event 6-11
Removing an Event 6-11
Viewing the Event Log 6-12
Traps 6-12
SPMA Trap Table Tool 6-13
Management Station 6-13
RMON Agent 6-14
Accessing the Trap Table Screen 6-15
Configuring the Trap Table 6-16

Chapter 7 Creating IndirectRMON Models

IndirectRMON Models 7-1
Creating an IndirectRMON Model 7-2
Placing an IndirectRMON Model into a View 7-3
The IndirectRMON Icon 7-4
IndirectRMON Information View Label 7-5
IndirectRMON Host Performance Label 7-6
The Off-Page Reference Icon 7-8
IndirectRMON Information View Label 7-8
IndirectRMON Host Performance View Label 7-8

Appendix A Ethernet Fields and Statistics

Ethernet Statistics Table A-1
Ethernet Statistics Detail View A-2
Frame Breakdown Chart A-2
Error Breakdown Chart A-3
Ethernet History Control Table A-4
History Table A-4
Hosts Control Table A-6
Host Table A-7
Host Table Detail A-8
Matrix Control Table A-9
Matrix Table A-9
HostTopN Control Table A-10
Top Hosts View A-11

Appendix B Token Ring Fields and Statistics

Mac-Layer Statistics Table B-1
Mac-Layer Statistics Detail View B-2
Isolating Errors Chart B-2
Non-Isolating Errors Chart B-2
Event Breakdown Chart B-3
Mac-Layer History Control Table B-4
Mac-Layer History Table B-4
Promiscuous Statistics Table B-7
Promiscuous Statistics Detail View B-8
Promiscuous History Control Table B-9
Promiscuous History Table B-9
Hosts Tables B-11
Matrix Tables B-11
HostTopN Tables B-11
Ring Station Control View B-11
Station Order Table B-12
Non-Isolating Errors B-12
Isolating Errors B-13

Appendix C SpectroWATCH

Watches C-1
Enabling Rmon Watches C-1
Modifying or Creating Watches C-2
Using Rmon Watches C-2
Logging Watches C-3
Ethernet Watches C-3
Token Ring Watches C-5

Appendix D Sample Profiles

Ethernet Profile D-1
Ethernet Profile Field Descriptions D-2
Token Ring Profile D-4
Token Ring Field Descriptions D-5
Using a Wildcard to Specify All Network Interfaces D-7

Appendix E Object Identifiers (OIDs)

etherStats E-1
historyControl E-2
etherHistory E-2
hostControl E-2
host E-4
hostTime E-4
matrixControl E-4
matrixSD E-5
matrixDS E-5
hostTopNControl E-5
hostTopN E-6
alarm E-6
event E-6
log E-7
tokenRingMLStats E-7
tokenRingPStats E-8
tokenRingMLHistory E-8
tokenRingPHistory E-9
ringStationControl E-10
ringStation E-10
ringStationOrder E-11
ringStationConfigControl E-11
ringStationConfig E-11
sourceRoutingStats E-12

Appendix F Reports

Report Description F-1
SetUp F-2
    Monitor Point F-2
    SpectroWATCH Logging F-2
Statistical Reports F-2
    Standard Reports F-3
    Custom Reports F-3
    Running Reports F-3
Sample Statistical Report Output File F-4

Index

Figures

Chapter 1 Introduction

Figure 1-1. Sample RMON Model Configuration 1-3

Chapter 2 Modeling RMON in SPECTRUM

Figure 2-1. Example of an EMME Model Configuration 2-6
Figure 2-2. EMME DevTop View 2-7
Figure 2-3. RMON Modeling Process 2-8
Figure 2-4. LAN Information View 2-10

Chapter 3 Loading and Unloading Profiles

Figure 3-1. RMON Profile Load/Unload View 3-2
Figure 3-2. Error Log File Entries 3-5

Chapter 4 Icons and Icon Components

Figure 4-1. RMONApp Icon 4-1
Figure 4-2. RMONApp Icon Subviews Menus 4-2
Figure 4-3. RMONEProbe Icon 4-4
Figure 4-4. RMONEProbe Icon Subviews Menu 4-5
Figure 4-5. RMONTProbe Icon 4-6
Figure 4-6. RMONTProbe Icon Subviews Menu 4-7

Chapter 5 Using RMON Views

Figure 5-1. Ethernet Statistics Table 5-4
Figure 5-2. Ethernet History Control Table View 5-7
Figure 5-3. Host Control Table View 5-8
Figure 5-4. Host Table View 5-10
Figure 5-5. Matrix Control Table View 5-11
Figure 5-6. Matrix Table View 5-12
Figure 5-7. HostTopN Control Table View 5-13
Figure 5-8. Top Hosts View 5-14
Figure 5-9. Mac-Layer Statistics Table 5-15
Figure 5-10. Promiscuous Statistics Table 5-17
Figure 5-11. Mac-Layer History Control Table View 5-19
Figure 5-12. Promiscuous History Control Table View 5-20
Figure 5-13. Ring Station Control View 5-22
Figure 5-14. Station Order 5-23

Chapter 6 Configuring RMON Alarms and Events

Figure 6-1. Alarm Table and Alarm Creation View 6-2
Figure 6-2. Alarm Set Up View 6-5
Figure 6-3. Event Table View 6-8
Figure 6-4. Event Set Up View 6-8
Figure 6-5. Event Log Table View 6-12
Figure 6-6. Trap Table Screen 6-15

Chapter 7 Creating IndirectRMON Models

Figure 7-1. IndirectRMON Creation View 7-2
Figure 7-2. IndirectRMON Icon 7-4
Figure 7-3. IndirectRMON Information View 7-5
Figure 7-4. IndirectRMON Host Performance Information 7-6
Figure 7-5. Performance Rates 7-7
Figure 7-6. Off-Page Reference Icon 7-8

Tables

Chapter 2 Modeling RMON in SPECTRUM

Table 2-1. SPECTRUM Model Type Designations 2-2

Preface

This manual describes the RMON Management Module, which allows you to collect, manage, and monitor information about a remote LAN segment.

Who Should Read This Manual

Read this manual if you are going to use the RMON Management Module to analyze networks that have been modeled in SPECTRUM. Before reading this document, you should be familiar with SPECTRUM's functions as described in the *SPECTRUM System User's Guide* and the *SPECTRUM System Administrator's Guide.*

How This Manual Is Organized

The *Management Module Guide for Standard RMON* is organized into the following chapters and appendices.

- Chapter 1—Introduces the RMON Management Module, its features, and its model types.
- Chapter 2—Explains how to model and configure RMON in SPECTRUM.
- Chapter 3—Describes how you can use the Profile Load/Unload facility to customize control table information.
- Chapter 4—Describes the icon components for the RMONApp, RMONEthProbe, and RMONTRProbe models.
- Chapter 5—Describes the Icon Subviews menu selections for RMON.
- Chapter 6—Explains how to configure RMON alarms and events.
- Chapter 7—Explains how to create IndirectRMON models.
- Appendix A—Describes Ethernet fields and statistics displayed in the RMON tables.
- Appendix B—Describes Token Ring fields and statistics displayed in the RMON tables.
- Appendix C—Describes SpectroWATCH's Watch Information report.

- Appendix D—Provides sample profiles for Ethernet and Token Ring.
- Appendix E—Provides object IDs (OIDs) that you supply during alarm creation.
- Appendix F—Describes the Report Information Block (.rib) files included with the RMON Management Module.

Related Reading

The following documents contain more information about remote monitoring, SPECTRUM, and TCP/IP-based networks.

SPMA Tools User's Guide, Cabletron Systems, Inc.

LAN Troubleshooting Handbook, Mark Miller, M&T Publishing, Inc., 1989.

SNMP, SNMP V2, and CMIP — The Practical Guide to Network Management Standards, William Stallings, Addison Wesley, 1993.

The Simple Book — An Introduction to Management of TCP/IP-based Internets, Marshall T. Rose, Performance Systems International, Inc.

Computer Networks, Andrew S. Tanenbaum, Prentice-Hall, Inc.

Local Area Networks, Architectures and Implementations, James Martin & Kathleen K. Chapman for the Arben Group, Inc., Prentice-Hall, Inc., 1989.

Questions about SPECTRUM Documentation

Send your questions, comments or suggestions regarding SPECTRUM documentation to the Technical Communications Department directly via the following internet address:

spectrum-techdocs@ctron.com

Chapter 1

Introduction

This chapter provides an introduction to the RMON Management Module and its model types.

RMON Management Module

A management module is a C++ coded software emulation of a physical device or software agent. The management module uses icons based on X Windows/ OSF Motif to represent this device in the user interface. Management module icons provide visual status at a glance through the use of various color definitions, as well as access to in-depth information on the device's configuration and operating activity. The management module software allows a network administrator to model, monitor, and manage individual devices or groups of devices on a network. The RMON Management Module supports RMON agents managed through the SNMP basic network management agent. SPECTRUM bases its device management on the Management Information Base (MIB) which comes as part of the management module.

The RMON Management Module and guide contain all the information necessary to manage RMON agents using SPECTRUM.

SPMA and RMON

The Remote Network Monitoring (RMON) feature provides a means of distributing network monitoring functions down through your network. RMON is an extension of the SNMP MIB that gives devices the ability to serve as micro-monitors for their segments of a network. They can collect, map, and sort detailed network statistics. RMON devices can monitor the performance of non-SNMP compliant and non-IP devices.

The SPECTRUM Portable Management Application (SPMA) software allows you to control and configure these capabilities, and allows you to access the network data collected by the RMON device.To access this view, highlight the

device icon, select ***View > Utilities > Applications***. Within the Applications dialogue box, click on the ***RMON Suite button***. For additional information about SPMA for RMON, refer to ***SPMA for Remote Network Monitoring User's Guide.***

SPECTRUM and RMON

Remote Network Monitoring, or RMON, was developed by the Internet Engineering Task Force (IETF) as a means of monitoring remote networks using the SNMP protocol. The resulting RMON MIB provides a uniform, standards-based framework that management stations can use to obtain performance data from an entire network segment.

RMON provides a means of distributing network monitoring functions down through the network to remote devices. Management station processing power and network bandwidth become freed up, and the overall efficiency of a local or wide-area network improves.

The SPECTRUM Remote Monitoring (RMON) Management Module monitors and manages RMON agents on remote LAN segments through the use of SPECTRUM's graphical user interface and Inductive Modeling Technology (IMT). Using the RMON Management Module, network administrators can check the performance of their remote network segments, gather statistics for problem identification and resolution, and diagnose network problems remotely. SPECTRUM can model any SNMP device that supports RMON. RMON devices can do the following:

- Collect a wide variety of detailed statistics for use in trend analysis
- Sort statistics by host for usage analysis
- Respond to user-defined thresholds applied to any of the statistical data

In addition, RMON devices provide extended monitoring capability. Because the RMON agent monitors every network device, it can track the performance of older devices that were previously inaccessible, such as those that are not compliant with SNMP. (For a list of supported devices, see *Devices That Support RMON* later in this chapter.)

RMON Models

Every network device has one or more network interfaces through which it connects to network segments, and thereby to the network. These interfaces are communications ports of the device which are physically connected to the network and carry network traffic to and from the device. An EMME, for example, has 4 network interfaces for connecting up to 4 separated and

distinct network segments, which are then internally bridged or routed within the EMME.

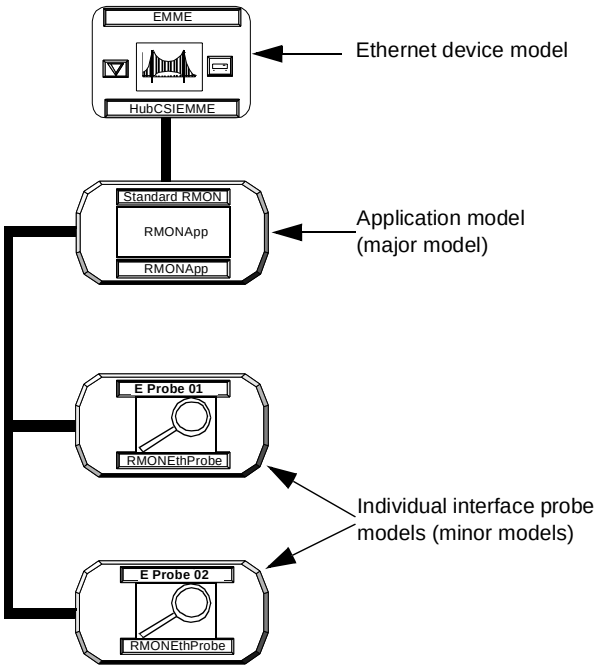
An RMON agent running on a network device collects and maintains RMON data for each interface on the device. The RMON Management Module supports three types of models to represent the RMON agent and its supported applications and interfaces. When you use SPECTRUM to model a device that supports RMON, RMON models are created automatically within SPECTRUM's Application View. The following sections provide a description of these models and their relationship to each other.

An **RMONApp model** accesses and presents RMON data from all network interfaces supported by a device. An **RMON probe model** accesses and presents RMON data specific to one interface. Depending on your network, the probe models are specific to Ethernet or Token Ring.

Icons for the RMONApp model and RMON probe model appear in SPECTRUM's Application View. Icons are graphical representations of the models that exist within the SPECTRUM database. From the icons, you can access SPECTRUM subviews that provide detailed RMON data collected on the network interfaces that the models represent.

Figure 1-1 shows a portion of an EMME's application view, showing the RMONApp model and probe models for two of the four interfaces on the device.

Figure 1-1. Sample RMON Model Configuration



Major Software Application Models

When a device is modeled, SPECTRUM automatically creates a model for each major software application (such as the RMONApp) that is present on the device. Major software application models appear in SPECTRUM's Application View in the first tier beneath the device model; black lines connect each major model directly to the device model. SPECTRUM associates major application models with the device model through the Model Type Editor's "Manages" relation. (For additional information about the Model Type Editor (MTE), see the *SPECTRUM Model Type Editor Guide*.) Information presented in the major application model is a summary of the minor software applications associated with it through the MTE's "Provides" relation. The RMONApp model represents the RMON MIB in the RMON device's application view.

Minor Software Application Models

When a device is modeled, SPECTRUM automatically creates a model for each minor software application (such as an RMON probe) that is present on the device. Minor software application models appear in SPECTRUM's Application View beneath the first tier of major models; black lines connect each minor model directly to its major model. SPECTRUM associates minor application models with the major software application models through the MTE's "Provides" relation.

- The RMONEthProbe model represents the RMON MIB in an Ethernet device's application view. SPECTRUM creates an RMONEthProbe model for each Ethernet interface supported by the device.
- The RMONTRProbe application model represents the RMON MIB in a Token Ring device's application view. SPECTRUM creates an RMONTRProbe model for each Token Ring interface supported by the RMON device.

A probe model can provide monitor point capabilities when pasted into a SPECTRUM 802.3 or 802.5 LAN segment model. Refer to Chapter 2 for instructions about how to designate a probe as a monitor point.

Device Models

The IndirectRMON device model, which you create, represents a physical device on the subnet known to the RMON agent through MAC address information located in the Host group. For further information, refer to Chapter 7, *Creating IndirectRMON Models*.

RMON Groups

- The RMON MIB, which is based on RFC 1271 (Ethernet) and RFC 1513 (Token Ring), is divided into the following groups:
- Statistics
- History
- Alarm
- Host
- HostTopN
- Matrix
- Filter
- Packet Capture
- Event
- Token Ring

Each group defines a set of objects to be monitored. In addition, each group stores data and statistics collected by the agent on the device, which may have multiple network interfaces.

Supported RMON Groups

The RMON Management Module currently supports the following RMON groups:

Group	Description
Statistics	Maintains low-level utilization and error statistics for each subnetwork monitored by the agent. Statistics include packet counts, error breakdown, and frame size breakdown.
History	Records periodic statistical samples over specified intervals.
Alarm	Monitors user-selected statistics and compares them to user-defined rising and falling thresholds, generating alarms when the thresholds are reached or exceeded.
Host	Maintains statistics associated with each host, or node, on the subnetwork. The agent discovers hosts automatically as the source and destination MAC addresses of good packets are recorded.
HostTopN	Contains the top-performing host statistics from a list based on parameters in the host table. You can use the statistics to identify trends, such as the top three error-producing nodes or the top ten traffic-producing nodes.
Matrix	Maintains statistics associated with each host pair, or source and destination addresses, on the subnetwork.

Event	Controls the generation and notification of events from the monitoring agent.
Token Ring	These subgroups provide monitoring functions for Token Ring: • Ring Station Group—Provides information about each station on the ring, as well as each ring being monitored. • Ring Station Order Group—Provides the order of stations on the monitored ring. • Ring Station Configuration Group—Actively manages stations on the ring. • Source Routing Group—Displays utilization statistics derived from source routing information.

Unsupported RMON Groups

The RMON Management Module currently does not support the Filter group and Packet Capture group.

Chapter 2

Modeling RMON in SPECTRUM

This chapter describes the SPECTRUM views that contain RMON models, how to model and configure devices that implement an RMON agent, and how to set up RMON as a network monitor point.

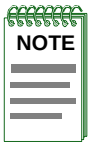
How to Model RMON

Modeling RMON in SPECTRUM involves the following steps:

- Creating models of devices that support RMON
- Enabling the RMON Host and Default MIB components for a modeled device
- Optionally selecting an RMON probe model as the monitor point for the SPECTRUM network model

Creating a Device Model That Supports RMON

When you model RMON, the first step is to create a device model that supports RMON.



If you are modeling a Cabletron device, (see *Enabling RMON for a Cabletron Device* on page 2-3) *for steps you may have to perform before you create a device model.*

Follow these steps to create a device model:

1. Navigate into SPECTRUM's Universe Topology View.
2. Select Edit from the File menu.
3. Select New Model from the Edit menu.

4. Select a model type that supports RMON from the Select Model Type dialog box.

   The following table lists RMON devices and their model type designations in SPECTRUM. If your device supports RMON but does not have a model type designation in SPECTRUM, use the GnSNMPDev model type.

Table 2-1. SPECTRUM Model Type Designations

RMON Device	Model Type
9E132-15	9E132-15
9E133-36	9E133-36
9E138-12	9E138-12
9E138-36	9E138-36
9E139-12	9E139-12
9E139-36	9E139-36
EMME	HubCSIEMME
EMM-E6	BRtrCSIEMM_E6
ESX1320	BRtrCSIESXW
ESXMIM	BRtrCSIESXM
NBR620	BRtrCSINBR620
MRXI 22/24	HubCSIMRXi
MicroMMAC-E	BRtrCSIuMMAC
MicroMMAC-T	BRtrCSIuMMACT
TRMM	HubCSITRMM
TRMM-2	HubCSITRMM2
TRMMIM	HubCSITRMMIM
TRXI	HubCSITRXi
Others	GnSNMPDev

   To support RMON, devices must be configured with certain firmware versions and memory resources. For more information about RMON requirements, contact Cabletron Systems Technical Support.

5. Click on OK. The Creation View dialog box for that device type appears.

6. In the model's Creation View dialog box, supply the following information:

   - **Model Name**—A unique name that identifies this device.
   - **Network Address**—The device's Internet Protocol (IP) address.

- **Community Name**—The Community Name assigned locally to this device. The default value is *public*. See your network administrator to verify that the Community Name has not been changed from *public* to another access policy name before modeling this device.
- **Location**—The location where the device is installed. This field is optional.
- **Contact**—The contact person or group who can provide troubleshooting help. This field is optional.
- **Serial Number**—The device's serial number.
- **Security String**— A SPECTRUM Security String for the device model.
- **Polling Interval**—The interval, in seconds, during which SpectroSERVER reads all attributes of the model that are flagged as POLLED. The default value is 60 seconds.
- **Log Ratio**—The number of poll cycles that must occur before SpectroSERVER records any attributes that are flagged as LOGGED. The default value is 10.

7. After entering the parameter information, click on OK. SPECTRUM places the icon representing the device at the top of the window. To move the icon to another area of the window, drag it with the left mouse button while still in Edit mode.

8. To exit Edit mode, select Save & Close from the File menu.

Enabling RMON for a Cabletron Device

In order for SPECTRUM's modeling process to detect RMON's presence and create the appropriate RMON models, you must enable the RMON Host and RMON Default MIB components on the device. In addition, you must verify that the community names for the Host and Default MIB components match the community names you used when you modeled the device.

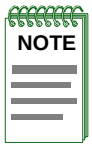
If these components are not enabled or their community names do not match the community names used when modeling the device, either of two things can happen:

- The RMON models will not appear in the device model's Application View
- The RMON models will not contain the entire set of RMON menu selections

If you suspect either of these problems has occurred on a device you have modeled, or if you want to verify these settings, you can access the component and community name information through the component table in the Configuration View of your device model.

Follow these steps to enable the MIB components and set the community names:

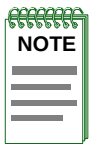
1. Click on Configuration in the device's Icon Subviews menu. The Device Configuration View appears.
2. Click on Component Table.
3. Deselect any preselected components in the Component Table.



When you enable any of the RMON components, you may need to upgrade your device's memory requirements to improve overall system performance. In addition, the RMON MIB's Matrix Group may not be supported if your device operates on less than 8 megabytes.

4. Select RMON Default.
5. If the Administrative Status is Disabled, set it to Enabled.
6. If the community name is incorrect, change it.
7. Repeat steps 3 through 6 for the RMON Host component, selecting RMON Host in step 4.

Do NOT disable any other selections in supported Cabletron Device Component Tables. This action may cause unexpected results for the device being modeled. td



After you enable the RMON Host component, you may notice a minor performance impact on bridging or routing functions. This happens because the RMON Host group locks some memory.

8. After reconfiguring the device's Component Table, you must reconfigure the SPECTRUM model. Follow these steps to reconfigure the model:
   a. From your model's Icon Subviews menu, select Model Information View.
   b. In the Model Information View, select Configure Model.

Now that you have created a model of the device and have enabled the RMON Host and Default MIB components, you have the option of configuring RMON to be a network monitor point. A monitor point is a device that collects statistical information from a network. The statistics are used to calculate total network activity.

Configuring RMON as a Network Monitor Point

When you work with RMON, you have the option of configuring an RMON probe model as a network monitor point for the given segment or ring. A monitor point is a device within a network group model (such as a LAN_802_3 or LAN_802_5 network) that provides the statistics that are used to calculate network activity in the network group model's Performance View. The specific monitor point device is selected by SPECTRUM based on the value of its Monitor Precedence attribute.

Within a network model, the device model having the highest Monitor Precedence value becomes the monitor point for that network group. If more than one device has the same Monitor Precedence value, the first device seen is chosen. Typically, the highest precedence value belongs to network analyzing devices, followed by successively less intelligent devices. You can modify default precedence values by updating them in a network's Information View.

As described below, to use RMON as a monitor point in a network model, you must first make a copy of an RMON probe and paste it into the network model. When you copy a probe model into a network model, an instance of the statistics group is automatically created on the device which the probe model represents. This instance is owned by the monitor point and provides the statistics for the monitor point feature. For more information about the statistics group, refer to Appendix A.

For Ethernet devices an instance of the Ethernet Statistics is created, and for Token Ring an instance of MAC Layer Statistics is created.

When the probe model is removed from the network model, the instances created for the monitor point are deleted.

To make RMON a network monitor point, you must accomplish these tasks:

- Associate the probe model with a network interface
- Copy the probe model into the network model at that interface
- Select the probe model as the monitor point

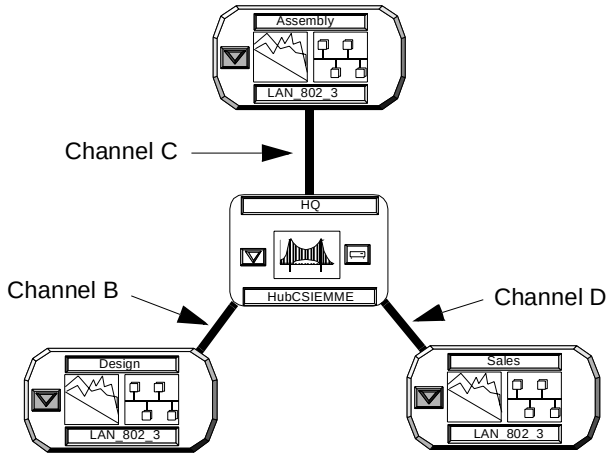
The following sections describe these modeling tasks.

Associating an RMON Probe Model with a Network Interface

The first step in making RMON a network monitor point is to associate the probe model with a network interface. An RMON probe model that monitors a network interface can be a monitor point only for the network connected to that interface.

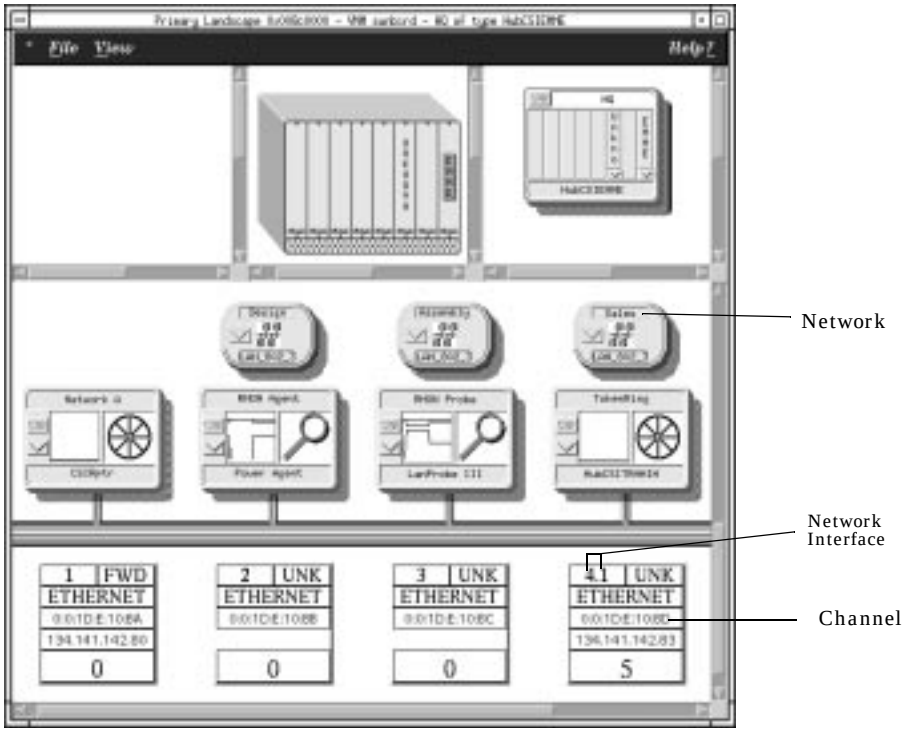
To understand how to identify the SPECTRUM network model at that interface, let's use the configurations shown in Figure 2-1 and Figure 2-2 as examples. Figure 2-1 depicts a typical network configuration of an EMME. Three of its network interfaces are dedicated to separate networks.

Figure 2-1. Example of an EMME Model Configuration



To find out which network interface is attached to each network, you need to inspect the DevTop view of the EMME model, shown in Figure 2-2.

Figure 2-2. EMME DevTop View



In Figure 2-2, three of the EMME's network interfaces are associated with a network model at that interface. For example, interface 2 is associated with the Design network model. Thus, using the information from the DevTop view, the RMON Probe models and the SPECTRUM network models are associated as follows:

Network Interface	Channel	Probe Model	Network Model
2	B	E Probe 02	Design
3	C	E Probe 03	Assembly
4	D	E Probe 04	Sales

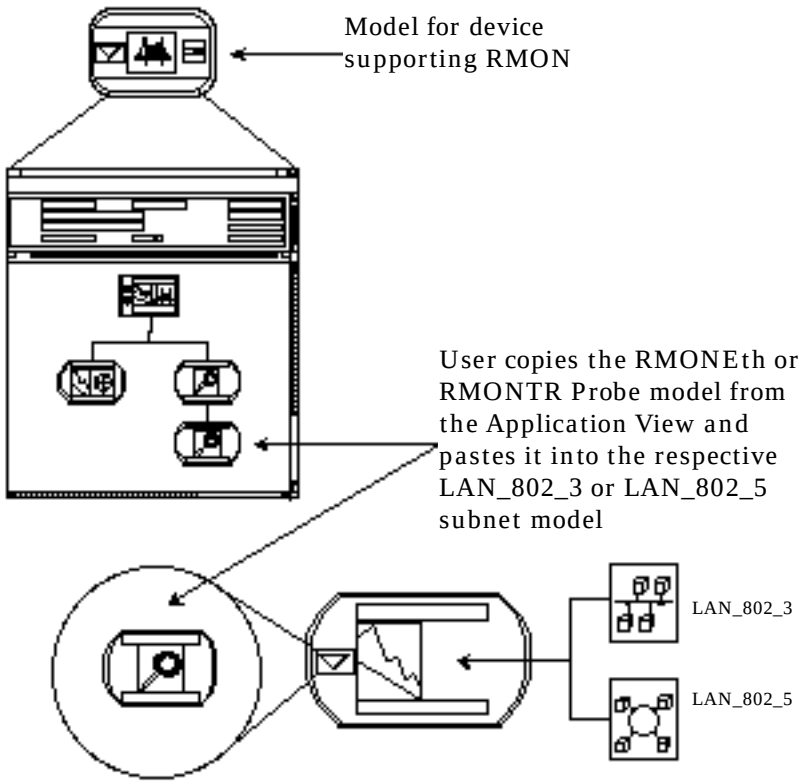
Copying RMON Probes into Network Models

To designate an RMON probe model as a monitor point, copy the RMON probe model from the device's Application View and paste it into the corresponding 802.3 or 802.5 network model. The RMON Probe becomes a monitor point device within that segment.

Follow these steps:

1. Open the Application View for the device you modeled.
2. Select Edit from the File Menu.
3. Highlight the probe that you want to copy.
4. Select Copy from the Edit Menu.
5. Open the Topology View for the discrete LAN.
6. Select Edit from the File Menu.
7. Select Paste from the Edit menu.

Figure 2-3. RMON Modeling Process

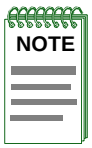

Model for device supporting RMON
User copies the RMONEth or RMONTR Probe model from the Application View and pastes it into the respective LAN_802_3 or LAN_802_5 subnet model
LAN_802_3
LAN_802_5

Verifying the Monitor Point

The last step in the monitor point process is to verify that the RMON Probe is selected as the monitor point for the LAN. If you configure the RMON Probe to be the monitor point device, RMON segment performance data is presented in the Performance View of the network model.

Within a network model, the device or probe model having the highest Monitor Precedence value becomes the monitor point for that network model. If more than one of these models has the same Monitor Precedence value, the first model created is chosen.

The RMON Ethernet and Token Ring probes have monitor precedence values of 60.

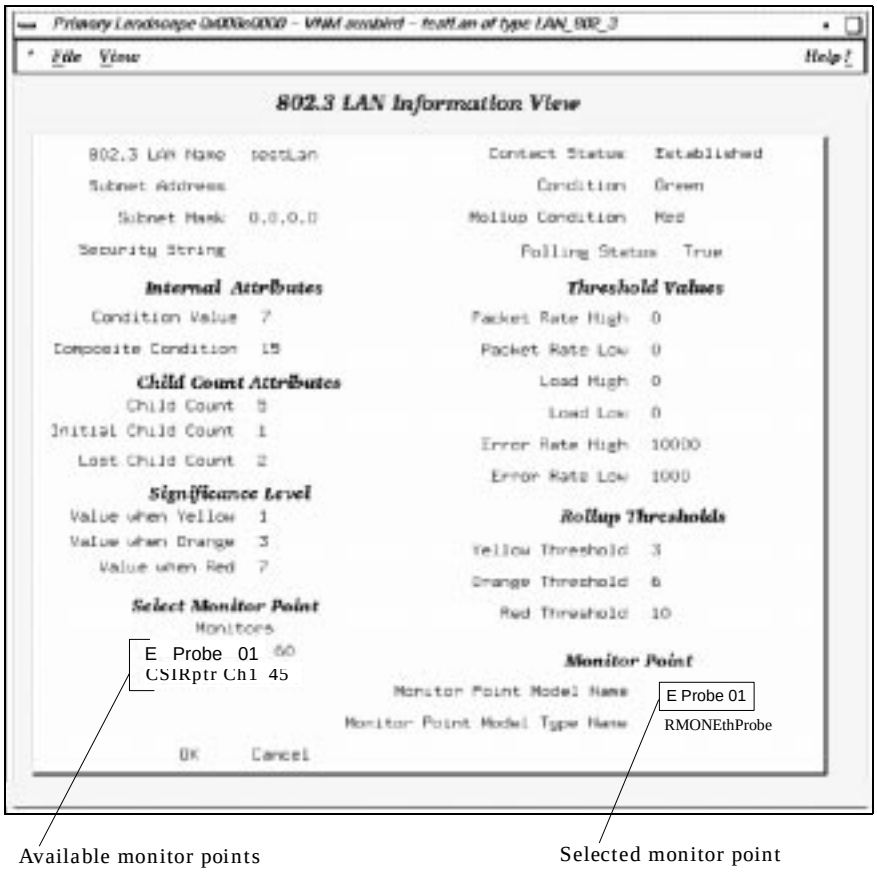


The RMONTRProbe application will not support monitor point capabilities if the Token Ring Mac-Layer or Promiscuous Statistics group is not supported by the device. Likewise, the RMONEthProbe application will not support monitor point capabilities if the Ethernet Statistics group is not supported by the device.

To verify that the RMON probe is the monitor point, perform the following steps:

1. Navigate to the Topology view that contains the network model.
2. Highlight the probe's network model by clicking on it.
3. Click the middle mouse button and select Information from the Icon Subviews menu. The LAN Information View appears (see Figure 2-4).
4. Verify that the values displayed in the monitor point information fields (located in the lower right portion of the view) indicate that the pasted Probe model is now the monitor point.

Figure 2-4. LAN Information View



To select a monitor point, or to modify an existing one, follow these steps:

1. Highlight the desired monitor point from the Select Monitor Point list and click OK.
2. Verify that the selected monitor point is now displayed in the Monitor Point Model Name field.

Chapter 3

Loading and Unloading Profiles

This chapter describes how to set up, load, and unload profiles.

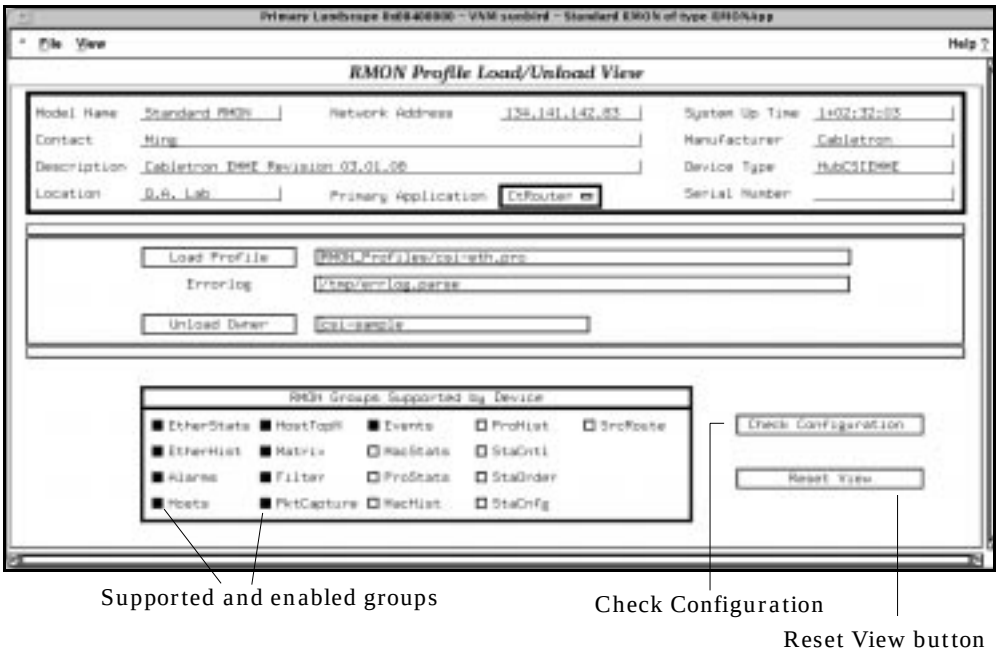
What is a Profile

Default control table instances of each RMON group are created on the device when the agent is started. In addition to these instances, you can download customized instances by using information stored in an ASCII file called a profile. Each profile specifies the control table characteristics you want to view. By using customized profiles, you can manually load and unload RMON control table information.

You can set up standard profiles in advance. You can download as many instances of each group as you like and are limited only by the resources available to the agent to support them. You can also remove instances. (Note that RMON Alarms/Events information cannot be loaded from profiles. Alarms and events must be created manually through the RMON Alarms/ Events View.)

To access the Profile Load/Unload View, select Profile Load/Unload from the RMONApp model's Icon Subviews menu. The Profile Load/Unload View shown in Figure 3-1 appears.

Figure 3-1. RMON Profile Load/Unload View



Checking Your Agent Configuration

The Profile Load/Unload View allows you to check which RMON groups are supported and enabled on the agent. You cannot, however, use this view to enable and disable the RMON groups themselves.

When you click on the Check Configuration button in the Profile Load/Unload View, the agent is queried for the RMON groups that are supported. Darkened buttons in the lower portion of the Profile Load/Unload View indicate those RMON groups that are supported and enabled. This action also updates the Icon Subviews menu of the RMON Application models for that agent, ensuring that the available menu selections match what is supported by the agent.

Note that the Reset View button only initializes the view; it has no effect on the agent at all.

Creating Custom Profiles

Cabletron provides starter files that you can use to create your own custom profiles. The starter files are located in the directory /*Spectrum_install_area*/SS/CsResource/RMON_Profiles. Note that the files are intended only as starter files; their configuration may not match your supported RMON groups or suit your needs.

See Appendix D for examples and descriptions of the format and syntax of profiles.

To create your own profile from one of the starter files, follow these steps:

1. Navigate to the default directory where the SPECTRUM profiles are located:

   cd /<***SPECTRUM_Directory_Path***>/SS/CsResource/RMON_Profiles

2. Copy the sample profile you want to use and give the copy a unique file name, as shown in the following example:

   cp csi-dflt.pro ***my-dflt.pro***

3. Edit the new profile with any text editor and customize the file according to the RMON configuration you want to load with the profile. You can include some or all of the RMON groups that are supported by your agent.

4. After all changes have been made, save the changes and then close the profile.

Loading Profiles

When you load a profile, the load process uses the **resource_file_path** parameter in your ss/.vnmrc file as the root path in its search for the specified profile.

By default, this parameter is set to the /***<Spectrum_Install_Area>***/SS/CsResource directory. Cabletron supplies an RMON_Profiles directory in this area, where you can find sample profiles and also store your custom profiles.

To load a profile, follow these steps:

1. Select the Profile Load/Unload View from the RMONApp model's Icon Subviews menu.
2. In the Profile File field, enter the path specification followed by your profile's name. Note that the path specification must be relative to the resource_file_path parameter specified in the ss/.vnmrc file. The following example shows the correct syntax for the default configuration:

   RMON_Profiles/***<profile_name>***
3. Ignore the OwnerString field. This field will be updated with information from the profile during the profile load process.
4. In the Errorlog field, enter a name for the error log file. This file will contain error log entries that occur during the profile load process. See the following section, *Problems When Loading Profiles*, for additional information about the error log file.
5. You must save your Profile View changes prior to loading, or they will have no effect. Click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears.
6. Click on Load Profile.

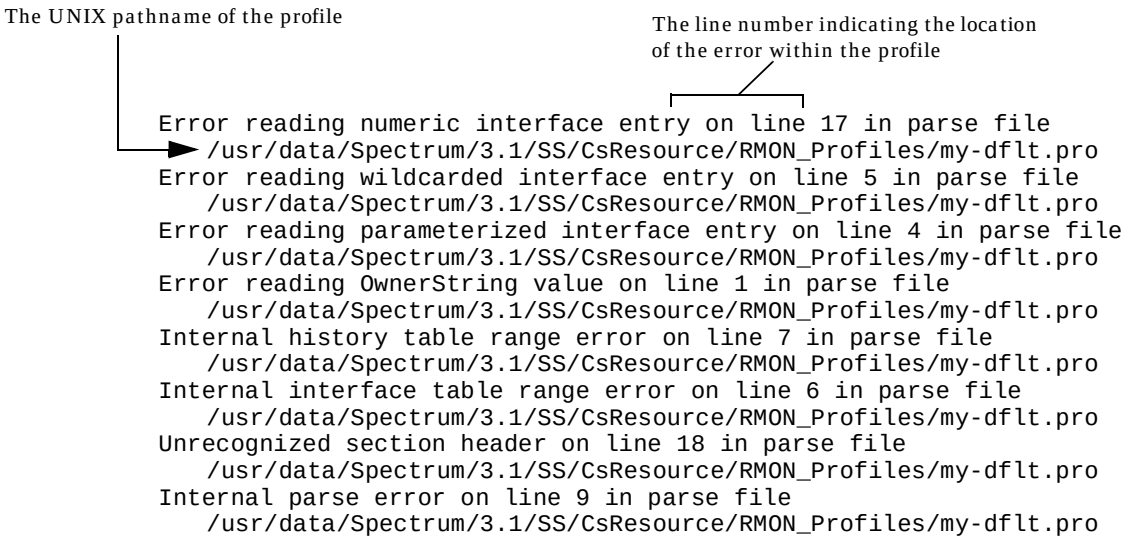
The message “Profile processing completed” indicates the profile has been evaluated and the agent has been loaded with the control table information. You can now go to any updated RMON group and view the new configuration.

If the message “Error accessing file” appears, close the message box and verify the accuracy of pathnames and file permissions. If you make any changes, be sure to save the updated information as described in Step 5.

Problems When Loading Profiles

When an error occurs while a profile is being loaded, the Profile Load/Unload parsing mechanism aborts the profile loading process, generates a parser error message that corresponds to the error, and records an error log entry in the error log file that you specified when you loaded the profile. Each error log entry includes a descriptive error message and the profile entry text that produced the error, as shown in the following examples.

Figure 3-2. Error Log File Entries


The UNIX pathname of the profile
The line number indicating the location of the error within the profile
Error reading numeric interface entry on line 17 in parse file
/usr/data/Spectrum/3.1/SS/CsResource/RMON_Profiles/my-dflt.pro
Error reading wildcarded interface entry on line 5 in parse file
/usr/data/Spectrum/3.1/SS/CsResource/RMON_Profiles/my-dflt.pro
Error reading parameterized interface entry on line 4 in parse file
/usr/data/Spectrum/3.1/SS/CsResource/RMON_Profiles/my-dflt.pro
Error reading OwnerString value on line 1 in parse file
/usr/data/Spectrum/3.1/SS/CsResource/RMON_Profiles/my-dflt.pro
Internal history table range error on line 7 in parse file
/usr/data/Spectrum/3.1/SS/CsResource/RMON_Profiles/my-dflt.pro
Internal interface table range error on line 6 in parse file
/usr/data/Spectrum/3.1/SS/CsResource/RMON_Profiles/my-dflt.pro
Unrecognized section header on line 18 in parse file
/usr/data/Spectrum/3.1/SS/CsResource/RMON_Profiles/my-dflt.pro
Internal parse error on line 9 in parse file
/usr/data/Spectrum/3.1/SS/CsResource/RMON_Profiles/my-dflt.pro

When the error message box is displayed, click on OK to close the message view. Review the error log file and then check your profile for syntax errors.

Unloading Profiles

Use the Profile Unload feature to remove default or user-configured instances from the agent Control Table and thereby free up resources on the device allocated to those instances.

When you remove profile information, you specify what to remove according to the owner of the instance. Therefore, the removal process is not group-specific; all instances in all groups associated with the specified owner will be removed.

To remove profile information, follow these steps:

1. Select the Profile Load/Unload View from the RMONApp model's Icon Subviews menu.
2. Ignore the Profile File field. (You need not modify this field.)
3. In the OwnerString field, specify the owner of the Control Table instances that you want to delete.
4. In the Errorlog field, enter a name for the error log file. This file will contain error log entries that occur during the profile unload process. See the previous section, *Problems When Loading Profiles*, for additional information about the error log file.
5. You must save your Profile View changes prior to unloading or they will have no effect. Click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears.
6. Click on Unload Owner. The profile information is removed from the Control Table.

The message "Profile processing completed" indicates the profile has been evaluated and the agent's control table information has been updated.

If the message "Error accessing file" appears, close the message box and verify the accuracy of pathnames and file permissions. If you make any changes, be sure to save the updated information as described in Step 5.

Chapter 4

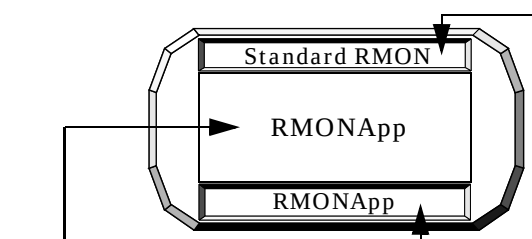
Icons and Icon Components

This chapter describes the RMON models and discusses how you can use the icons (the RMONApp icon, the RMON Ethernet probe icon, and the RMON Token Ring probe icon) to obtain network performance data.

The RMONApp Icon

The RMONApp icon (Figure 4-1) serves as a central gathering point for network device information and allows you to easily access data collected from multiple interfaces on the device. Each RMONApp icon represents a composite of the information gathered by all of the Ethernet or Token Ring probes that belong to its model. The icon features three labels that provide quick access to detailed information about the model. To access the information, double click on the label, using the left mouse button. (You can also access this same information through the Icon Subviews menu.)

Figure 4-1. RMONApp Icon



Model Information View label

This label displays the default or user-defined model name. Double click here to access the detailed Model Information View.

Contact Status Label

The label color reflects the device's contact status.

Profile Load/Unload View label

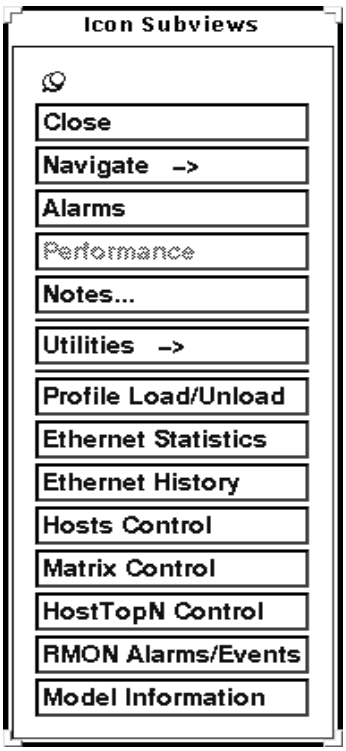
This label displays the model type name (RMONApp). Double click here to open the Profile Load/Unload View. The Profile Load/Unload feature allows you to control the categories that RMON monitors. Refer to Chapter 3 for detailed information about the Profile Load/Unload function.

RMONApp Icon Subviews

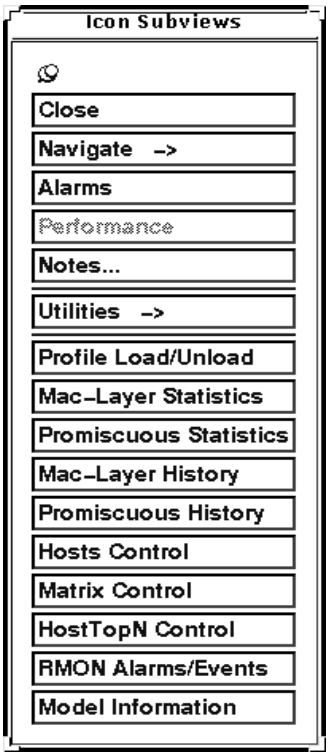
Icon subviews provide detailed information about the RMONApp model. To access the Icon Subviews menu, click the middle mouse button anywhere on the icon. As an alternative, you can click on the RMONApp icon to highlight it and then select Icon Subviews from SPECTRUM's View menu.

Figure 4-2. RMONApp Icon Subviews Menus

Ethernet Icon Subviews Menu



Token Ring Icon Subviews Menu



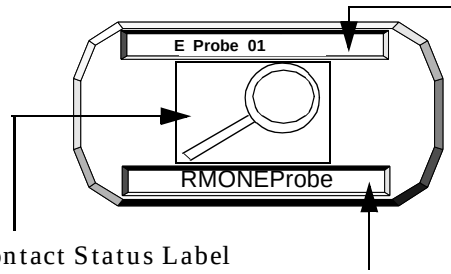
The following list briefly describes menu selections for the Ethernet and Token Ring RMONApp icons. Note that some menu selections describe options that are topology-specific; for example, menu selections for Ethernet are not available on a Token Ring network and vice versa. Chapter 5 describes the menu selections in more detail. Appendices A and B provide additional information about the statistics displayed by the menu selections.

Selection	Description
Close	Close the Icon Subviews menu.
Navigate	Move to a view higher or lower in the topology hierarchy.
Alarms	View alarms for the model.
Notes	Open the Notes facility.
Utilities	Open the utilities submenu.
Profile Load/Unload	Open the Profile Load/Unload View.
Ethernet Statistics	View Ethernet statistics for each interface on the device. (Ethernet only)
Mac-Layer Statistics	View a list of Mac-layer Token Ring statistics for each interface on the device. (Token Ring only)
Promiscuous Statistics	View a list of Promiscuous Token Ring statistics for each interface on the device.
Ethernet History	View Ethernet statistics for each interface.
Mac-Layer History	View Mac-layer Token Ring statistics for each interface, gathered at user-specified intervals. (Token Ring only)
Promiscuous History	View Promiscuous Token Ring statistics for each interface.
Hosts Control	View network traffic statistics associated with each host on the network segment for each interface on the device.
Matrix Control	View network traffic statistics associated with each host communication pair on the network segment for each interface on the device.
HostTopN Control	View top-performing host statistics on the network for each interface on the device.
RMON Alarms/Events	View and control RMON alarms and events.
Model Information	View configuration information about the model.

The RMON Ethernet Probe Icon

The RMON Ethernet probe (RMONEProbe) gathers statistics from a single interface on an Ethernet device. The RMONEProbe icon (Figure 4-3) contains labels that provide access to detailed information about the model. For quick access to the information, double click on the label, using the left mouse button. (You can also access this same information through the Icon Subviews menu.)

Figure 4-3. RMONEProbe Icon



Model Information View label

This label displays the default or user-defined name. The default name corresponds to the network interface with which this probe is associated. Double click here to access the detailed Model Information View.

Contact Status Label

The label color reflects the probe's contact status.

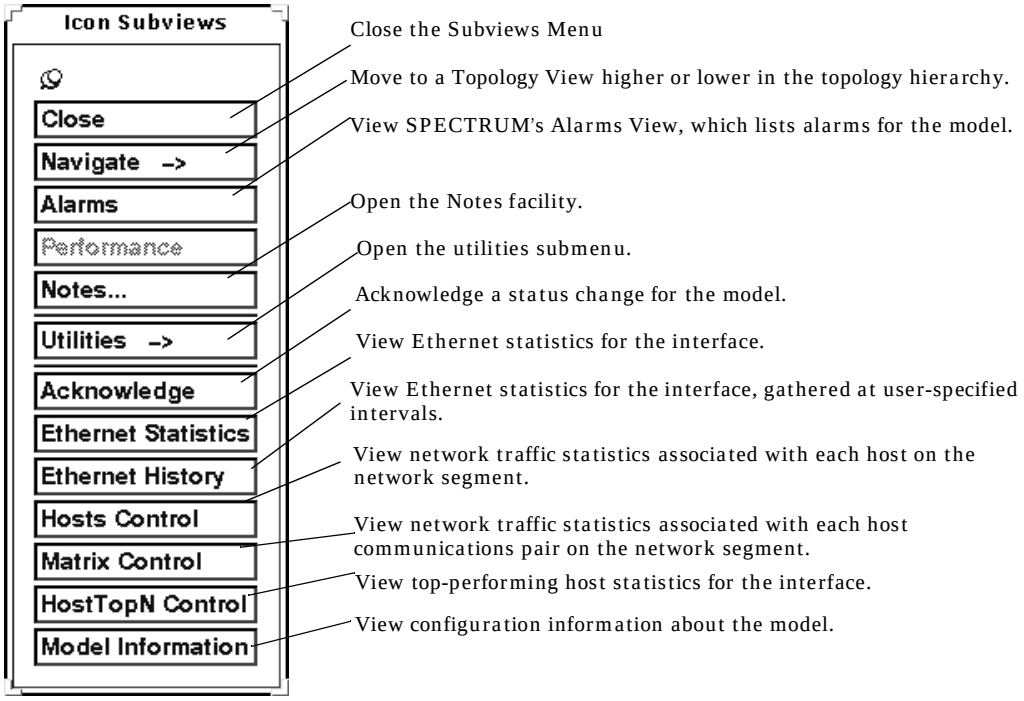
Ethernet Statistics Table View label

This label displays the model type name (RMONEProbe). Double click here to open the RMON Ethernet Statistics Table View. The table lists Ethernet statistics entries measured by the probe at its associated network interface. See Appendix Afor detailed information about these statistics.

RMONEProbe Icon Subviews

Click the middle mouse button anywhere on the RMONEProbe icon to access the Icon Subviews menu, shown in Figure 4-4. As an alternative, you can click on the RMONEProbe icon to highlight it and then select Icon Subviews from SPECTRUM's View menu.

Figure 4-4. RMONEProbe Icon Subviews Menu

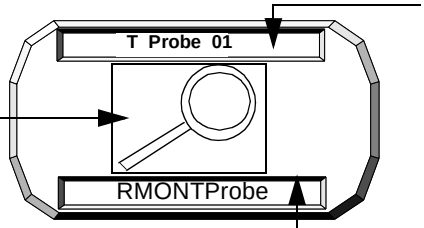

Icon Subviews
Close
Navigate –>
Alarms
Performance
Notes...
Utilities –>
Acknowledge
Ethernet Statistics
Ethernet History
Hosts Control
Matrix Control
HostTopN Control
Model Information
Close the Subviews Menu
Move to a Topology View higher or lower in the topology hierarchy.
View SPECTRUM's Alarms View, which lists alarms for the model.
Open the Notes facility.
Open the utilities submenu.
Acknowledge a status change for the model.
View Ethernet statistics for the interface.
View Ethernet statistics for the interface, gathered at user-specified intervals.
View network traffic statistics associated with each host on the network segment.
View network traffic statistics associated with each host communications pair on the network segment.
View top-performing host statistics for the interface.
View configuration information about the model.

From this menu, you can select one of many subviews that present detailed information about the model. The menu selections are described in more detail in Chapter 5. Appendix Aprovides additional information about the statistics displayed by the menu selections.

The RMON Token Ring Probe Icon

The RMON Token Ring probe (RMONTProbe) gathers statistics from a single interface on a Token Ring device. The RMONTProbe icon (Figure 4-5) contains labels that provide quick access to detailed information about the model. For quick access to the information, double click on the label, using the left mouse button. (You can also access this same information through the Icon Subviews menu.)

Figure 4-5. RMONTProbe Icon



Model Information View label

This label displays the default or user-defined name. The default name corresponds to the network interface with which this probe is associated. Double click here to access the detailed Model Information View.

Contact Status Label

The label color reflects the probe's current contact status.

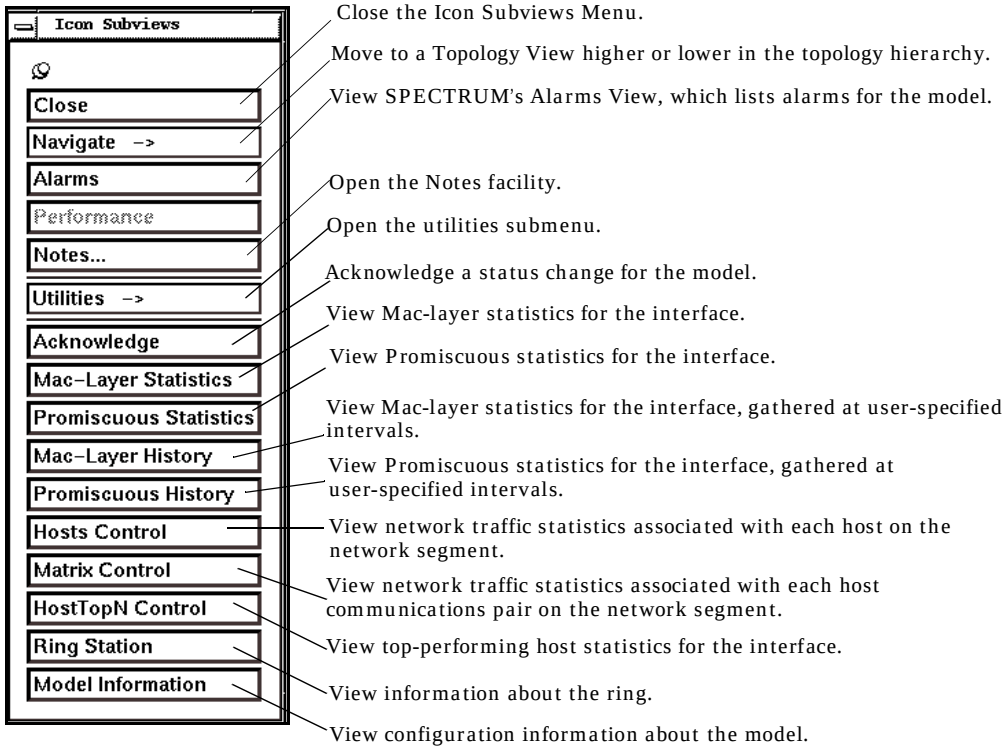
Mac-Layer Statistics Table View label

This label displays the model type name (RMONTProbe). Double click here to open the RMON Mac-Layer Statistics Table View. The table lists Token Ring statistic entries measured by the probe at its associated network interface. The statistics are free running counters that start at zero when a valid entry is created. See Appendix B for detailed information about these statistics.

RMONTProbe Icon Subviews

Click the middle mouse button anywhere on the RMONTProbe icon to access the Icon Subviews menu, shown in Figure 4-6. As an alternative, you can click on the RMONTProbe icon to highlight it and then select Icon Subviews from SPECTRUM's View menu.

Figure 4-6. RMONTProbe Icon Subviews Menu


Icon Subviews
Close
Navigate ->
Alarms
Performance
Notes...
Utilities ->
Acknowledge
Mac-Layer Statistics
Promiscuous Statistics
Mac-Layer History
Promiscuous History
Hosts Control
Matrix Control
HostTopN Control
Ring Station
Model Information
Close the Icon Subviews Menu.
Move to a Topology View higher or lower in the topology hierarchy.
View SPECTRUM's Alarms View, which lists alarms for the model.
Open the Notes facility.
Open the utilities submenu.
Acknowledge a status change for the model.
View Mac-layer statistics for the interface.
View Promiscuous statistics for the interface.
View Mac-layer statistics for the interface, gathered at user-specified intervals.
View Promiscuous statistics for the interface, gathered at user-specified intervals.
View network traffic statistics associated with each host on the network segment.
View network traffic statistics associated with each host communications pair on the network segment.
View top-performing host statistics for the interface.
View information about the ring.
View configuration information about the model.

From this menu, you can select one of many subviews that present detailed information about the model. describes the menu selections in more detail. Appendix B provides additional information about the statistics displayed by the menu selections.

Chapter 5

Using RMON Views

This chapter describes the RMON views that are available from the Icon Subviews menu. It also describes how you can tailor many of the views to suit your needs.

Views Unique to RMON

This chapter describes the views that are unique to the RMON management module.

To access the RMON views, highlight the RMONApp or RMON probe icon. Then click the middle mouse button anywhere on the icon; the Icon Subviews menu appears. As an alternative, click on View New View Icon Subviews.

The following table lists views that are unique to RMON. These views are described later in this chapter. Note, however, that the Profile Load/Unload view is described fully in Chapter 3 while the RMON Alarms/Events are described in Chapter 6.

The table indicates the network topology that supports each view and also identifies the RMON group on which the view is based. Note that some views appear only on an Ethernet network, while others appear only on a Token Ring network.

RMON View	Ethernet	Token Ring	RMON Group
Profile Load/Unload	3	3	N/A
Ethernet Statistics	3	—	Statistics
Mac-Layer Statistics	—	3	Statistics
Promiscuous Statistics	—	3	Statistics
Ethernet History	3	—	History
Mac-Layer History	—	3	History
Promiscuous History	—	3	History
Hosts Control	3	3	Host
Matrix Control	3	3	Matrix
HostTopN Control	3	3	HostTopN
Ring Station	—	3	Token Ring
RMON Alarms/Events	3	3	Alarms & Events

Customizing the RMON Tables

Many RMON tables share a common format and have identical options that you can use to customize the information output. The customization options are described in the following table.

Click on...	To...
The popup menu next to Sort ON	Sort table contents incrementally according to the entry type. The default is No Sort. Popup menu choices differ for each RMON table. When used in conjunction with Find, the sort preference also specifies the type of entry to be searched for. Sorted tables remain sorted when a table is updated.
Find	Find a value in the column specified by the sort preference. To locate a specific table entry, enter the value to be searched for in the popup dialog box. If the Find button is grayed-out, the functionality is unsupported.
Print	Export the data to an ASCII file. A dialog box prompts you to enter a name for the output file.
Update	Update the table's contents.
The popup menu next to Order	Sort table interfaces and statistics by ascending or descending order.

Loading and Unloading Profiles

The Profile Load/Unload View allows you to manually load and unload RMON control table information that is stored in a file called a profile. This subview selection is available only from the RMONApp model. Refer to Chapter 3 for detailed information about how to create, load, and unload RMON profiles.

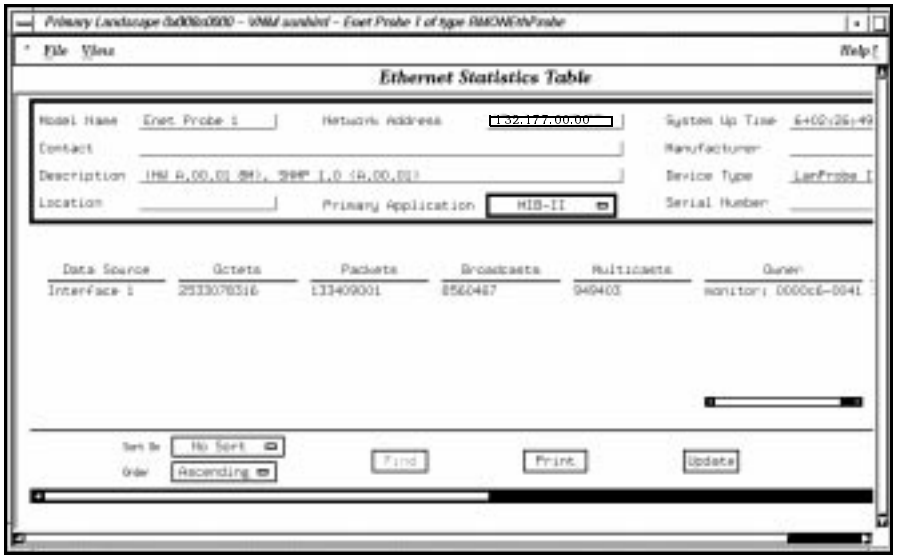
Accessing Ethernet Views

The following sections describe RMON views that appear on Ethernet icons. Refer to Appendix A for detailed descriptions of statistics that appear in Ethernet views.

Ethernet Statistics

From the Icon Subviews menu, click on Ethernet Statistics. The Ethernet Statistics Table shown in Figure 5-1 presents the RMON Statistics data in tabular form.

Figure 5-1. Ethernet Statistics Table



The RMON Statistics group consists of 17 parameters measured at the monitored network interface (data source) of the device. These statistics take the form of free running counters that start from zero when a valid instance is created. The Ethernet Statistics Table presents 13 of these parameters (briefly described below) but does not include detailed size distribution, which is presented in the Statistics Detail View described later in this section.

- **Data Source**—The interface being monitored.
- **Octets**—Total octets received.
- **Packets**—Total packets received.
- **Broadcasts**—Good packets received that were directed to a broadcast address.
- **Multicasts**—Good packets received that were directed to a multicast address.
- **Owner**—The person who configured the entry.
- **CRC/Align**—Total packets received that had a length of between 64 and 1518 octets, but were not an integral number of octets in length or had a bad FCS.
- **Collisions**—Best estimate of total number of collisions on this segment.

- **Fragments**—Total packets received that were not an integral number of octets in length or that had a bad FCS, and were less than 64 octets in length.
- **Jabbers**—Total packets received, longer than 1518 octets, and not an integral number of octets in length or with a bad FCS.
- **Oversize**—Total packets received, longer than 1518 octets, otherwise well-formed.
- **Undersize**—Total packets received, less than 64 octets long, otherwise well-formed.
- **Drop Events**—Total events in which packets were dropped due to lack of resources.

Viewing Performance Statistics on the Segment

Double click on any instance (row or interface) in the Ethernet Statistics table to view the RMON data presented in standard SPECTRUM Performance View format. This allows you to view current percentage calculations and a time graph of the interface activity, rather than the absolute numbers of the Statistics Table. Note that this view is dynamically updated.

Viewing Network Activity with the Multi-Attribute Line Graph

The Multi-Attribute Line Graph provides a general indication of network activity. The attributes' colors represent different statistics. Green represents Load, blue represents the Frame Rate, orange represents the Error Rate, and yellow represents Collisions.

You can scroll back in time to view previously logged values for these attributes.

Use the graph properties button to modify the presentation of the graph. It has three options:

- Scroll to Date-Time—sets the viewing area to begin at a specified date and time.
- Change Time Scale—sets the Y axis time scale for the graph.
- Data Logging—data logging is not relevant for the Segment Performance Views of the RMON Probe models.

Use the Lin/Log toggle button to toggle between a linear and a logarithmic scale presentation of the graph.

Viewing Statistics with the Details Button

Click the Details button in the Performance View for more diagnostic detail. The Statistics Detail View appears; it presents a graphical breakdown of the frame size distribution and error statistics which are updated and presented as totals or deltas. Note that this view is dynamically updated.

The Frame Breakdown pie chart provides a color-coded view of the network segment's total traffic by frame size, separated into the following categories:

- Undersize
- 64 Bytes
- 65 to 127 Bytes
- 128 to 255 Bytes
- 256 to 511 Bytes
- 512 to 1023 Bytes
- 1024 to 1518 Bytes
- Oversized
- Total

The Error Breakdown pie chart provides a color-coded view of the network segment's error types (Alignment, Collisions, Fragments, and Jabbers). Click on the Total, Delta, or Accum buttons to modify the data output.

- Total—The parameter's value over this instance's entire interval.
- Delta—The parameter's value over the duration of the update interval.
- Accum—The parameter's value over the interval since the Accum button was selected.

Ethernet History

From the Icon Subviews menu, click on Ethernet History. The Ethernet History Table presents the RMON History data in tabular form. The RMON History group records data from the Statistics group over user-defined intervals and stores it for later retrieval, allowing you to perform trend analysis of a statistic over time or to isolate periods of time during which a network event may have occurred.

Figure 5-2. Ethernet History Control Table View

The History Control Table (Figure 5-2) presents the configuration of each History instance running on the network interface. By default, the RMON standard specifies 2 instances, having intervals of 1800 seconds and 30 seconds. Each instance features the following fields:

- **Data Source**—Interface being monitored
- **Interval**—The sample collection interval
- **SizeReq**—Maximum number of recorded intervals (buckets) requested for the sample
- **Size**—The number of buckets currently recorded in the sample
- **Owner**—The person who configured the entry
- **Status**—The status of the control table entry

Note that when the values for SizeReq and Size are identical, the oldest entries in the History Control Table for that instance will be replaced by the newest entries.

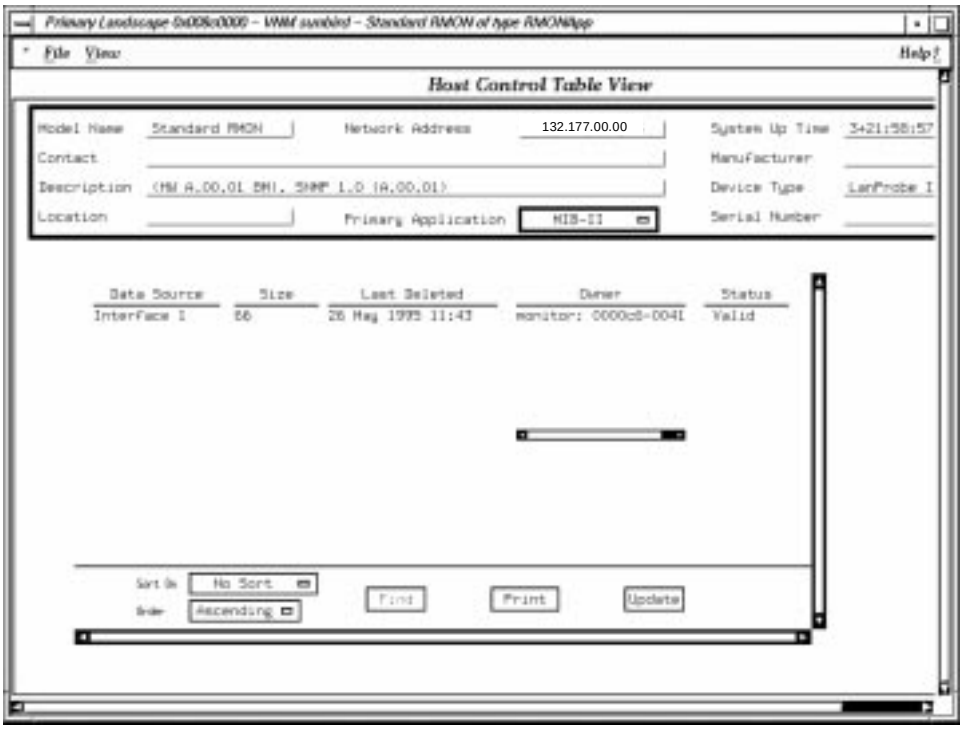
Viewing the History Table

Double click any History Control Table entry to display the data for that instance. The History Table shows the past performance measured at the monitored network interface (data source) of the device. Appendix A contains detailed descriptions of the fields found in the History Table.

Hosts Control

From the Icon Subviews menu, click on Hosts Control. The Hosts Control Table presents the RMON Host data in tabular form. The RMON Host group provides a breakdown of traffic statistics per network host by using the source and destination MAC address fields contained in a transmitted packet. This allows you to view the statistical data associated with each host and isolate traffic patterns per host, including items such as traffic levels and error levels.

Figure 5-3. Host Control Table View



The Host Control Table (shown in Figure 5-3) presents the configuration of each Host instance running on the network interface. Each instance features the following fields:

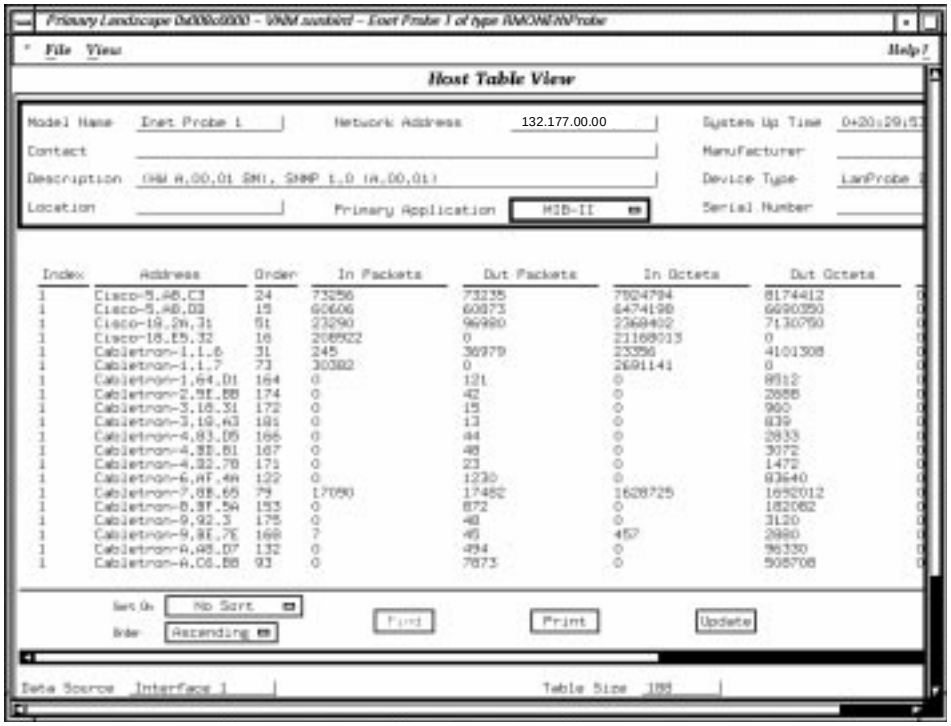
- **Data Source**—The interface being monitored.
- **Size**—The number of host entries in the table.
- **Last Deleted**—The time that the oldest entry was deleted and replaced by the newest entry.
- **Owner**—The individual or entity that configured this entry.
- **Status**—The status of this control table entry.

The number of entries in the table (Size) is allotted dynamically according to the resources available. This means that the oldest entry is deleted and replaced by the newest entry when there is a resource constraint; the time this occurs is indicated by the column Last Deleted.

Viewing the Host Table

Double click on any instance in the Host Control Table to open the Host Table View. The Host Table, shown in Figure 5-4, displays per-host traffic statistics measured at the monitored network interface (data source) of the device. Appendix A contains detailed descriptions of the fields found in the Host Table.

Figure 5-4. Host Table View



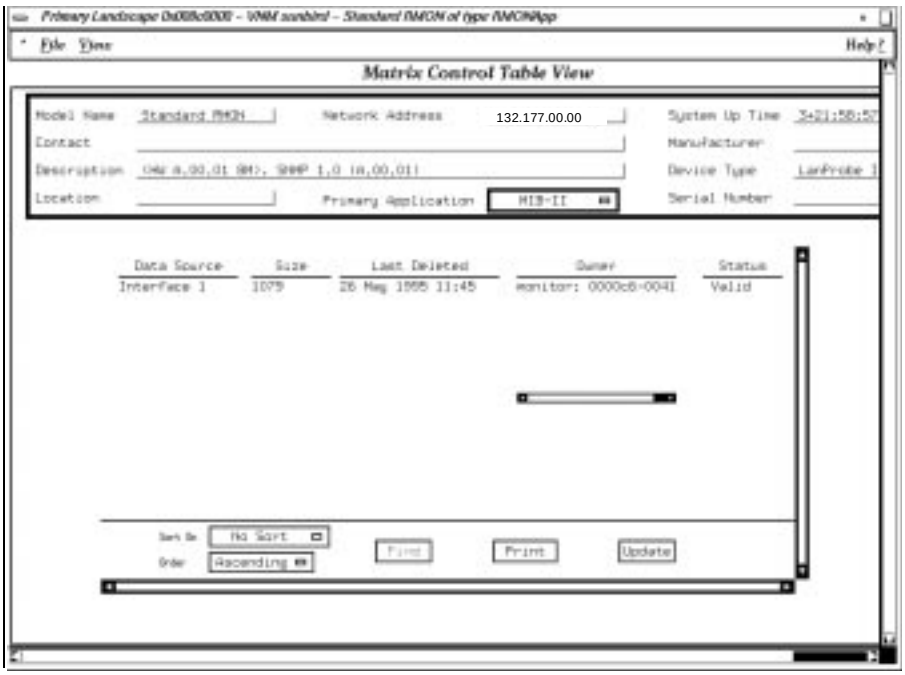
Viewing the Host Table Detail

Double click on any row in the Host Table to open the Host Table Detail for that MAC address. This screen displays many of the same categories that are found in the Host Table. In addition, if you click on the Create Indirect Model button, you can create a SPECTRUM model for the device at this MAC address. See Chapter 7, *Creating IndirectRMONs Models*, for more information about this task.

Matrix Control

From the Icon Subviews menu, click on Matrix Control. The Matrix Control Table presents the RMON Matrix data in tabular form. The RMON Matrix group provides a breakdown of traffic statistics according to the communication pairs it identifies on the segment by using the source and destination MAC address fields contained in a transmitted packet. You can view the statistical data associated with each host pair and isolate traffic patterns between pairs, such as traffic levels, error levels, etc. This information can be useful when characterizing the load distribution of the segment and when designing your network for proper load balance.

Figure 5-5. Matrix Control Table View



The Matrix Control Table (Figure 5-5) presents the configuration of each Matrix instance running on the network interface. For each data source, the Matrix Control Table shows the following items.

- **Data Source**—The interface being monitored.
- **Size**—The number of matrix entries in the table
- **Last Deleted**—The date that the last entry was deleted.
- **Owner**—The individual or entity that configured the entry.
- **Status**—The status of this control table entry.

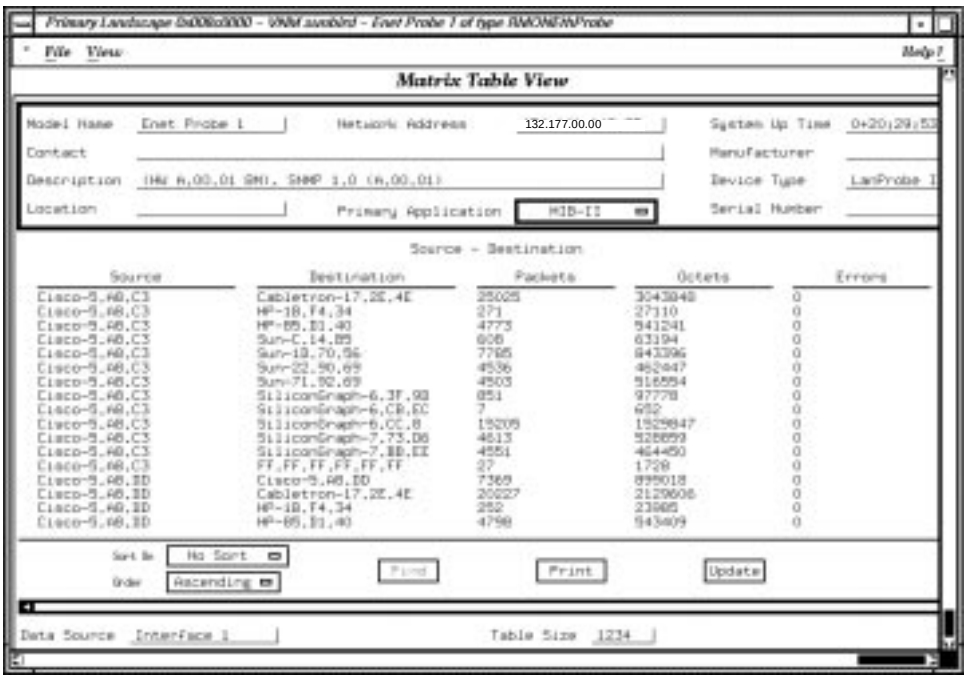
Note that size (the number of entries in the table) is allocated dynamically according to the resources available. When there is a resource constraint, the

oldest entry is deleted and replaced by the newest entry; the time this occurs is indicated by the column Last Deleted.

Viewing the Matrix Table

Double click on any instance in the Matrix Control Table to open the Matrix Table View. The Matrix Table View, shown in Figure 5-6, displays traffic statistics for each host pair, measured at the monitored network interface.

Figure 5-6. Matrix Table View



The following fields appear in the Matrix Table:

- **Source**—The source MAC address of communications for this pair.
- **Destination**—The destination MAC address of communications for this pair.
- **Packets**—The packets transmitted between the communicating hosts.
- **Octets**—The octets transmitted between the communicating hosts.
- **Errors**—The errors detected during communications between the hosts.

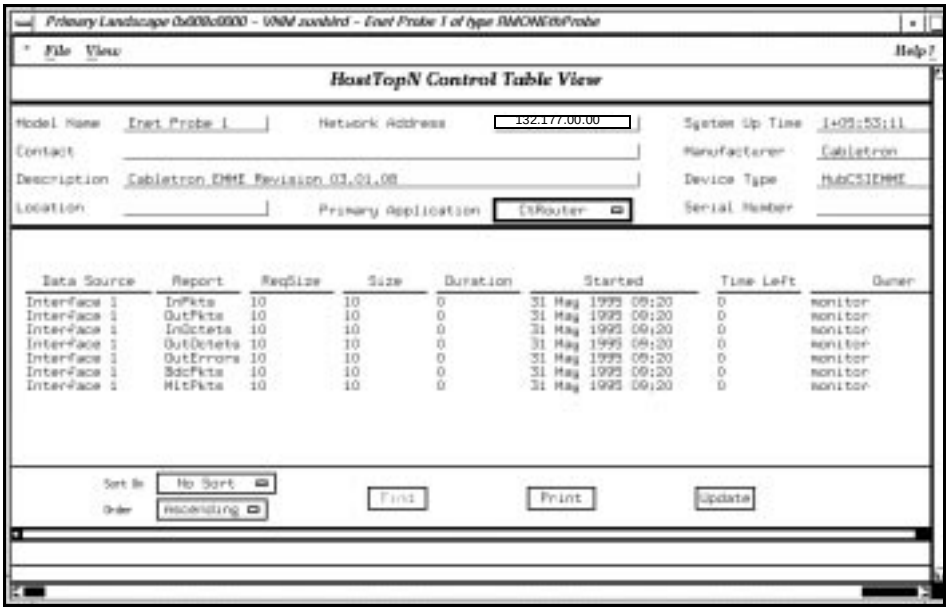
The source-destination table provides a complete cross-reference of source (transmitting) and destination (receiving) devices over the network segment. Note that addresses are translated to reveal the device's manufacturer.

HostTopN Control

From the Icon Subviews menu, click on HostTopN Control. The HostTopN Control Table (Figure 5-7) presents the RMON HostTopN data in tabular form. The RMON HostTopN group allows you to select one of the seven Host group statistics and determine an arbitrary number of hosts on the segment with the greatest value for that parameter.

You can specify the number of hosts included in a measurement, as well as the interval over which the measurement is made.

Figure 5-7. HostTopN Control Table View



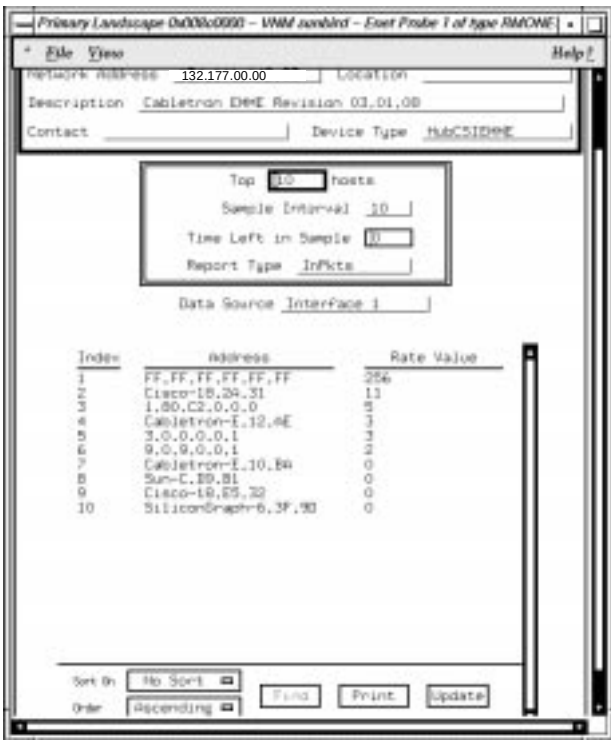
The HostTopN Control Table presents the configuration of each HostTopN instance running on the network interface. Fields for each data source include these items:

- **Data Source**—The interface being monitored.
- **Report**—The Host group statistic on which to perform the measurement.
- **ReqSize**—The number of hosts requested for this HostTopN measurement.
- **Size**—The number of hosts detected during the measurement interval.
- **Duration**—The interval in seconds requested for this HostTopN measurement.
- **Started**—The time this measurement interval started collecting data.
- **Time Left**—The number of seconds left in the measurement interval.
- **Owner**—The entity that configured this entry.

Viewing or Configuring the Top Hosts

To configure an instance of Top Hosts or to view the result of an instance or one in progress, double click on an instance listed in the HostTopN Control Table. The Top Hosts view (shown in Figure 5-8) appears, where you specify the measurement parameters and view the results of the completed sample. Use this view to determine (for example) which hosts are generating the most traffic, which are receiving the most traffic (in either packets or bytes), and which are generating the largest number of errors.

Figure 5-8. Top Hosts View



In the dialog box, enter the number of hosts to be included in the sample (Top hosts) and the duration of the sample (Time Left in Sample). Press Return and click OK in the Save Changes dialog box. The Top Hosts dialog box counts down the time left in the sample (Sample Interval) and notes the statistic being monitored (Report Type). Click Update to see the results, which are listed below the Top Hosts dialog box.

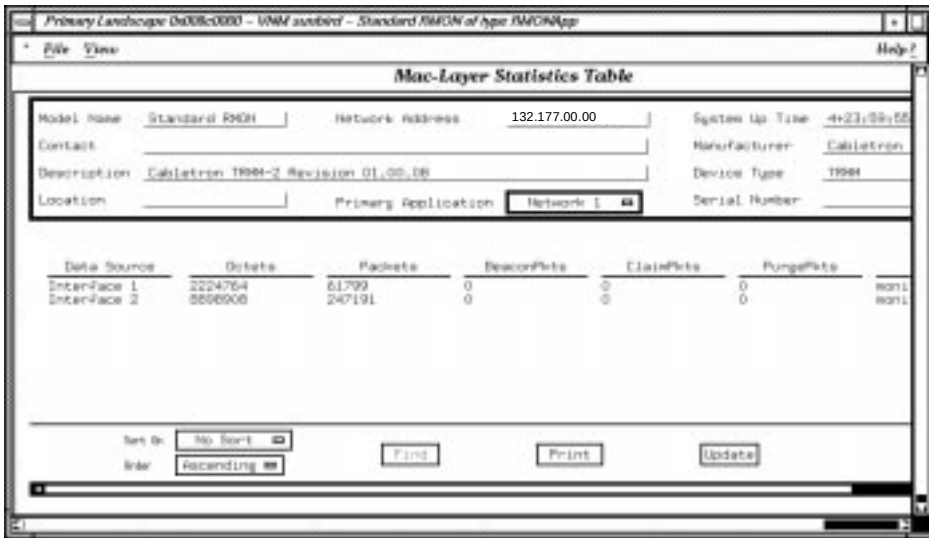
Accessing Token Ring Views

The following sections describe RMON views that appear on Token Ring icons. Refer to Appendix B, *Token Ring Fields and Statistics*, for detailed descriptions of statistics that appear in Token Ring views.

Mac-Layer Statistics

From the Icon Subviews menu, click on Mac-Layer Statistics. The Mac-Layer Statistics Table (Figure 5-9) presents the RMON statistics in tabular form.

Figure 5-9. Mac-Layer Statistics Table



The RMON Statistics group consists of the following 7 parameters measured at the monitored network interface (data source) of the device. These statistics take the form of free running counters that start from zero when a valid instance is created.

- **Data Source**—The interface being monitored.
- **Octets**—Total octets of data in MAC packets (excluding those that were not good frames) received on the network.
- **Packets—**Total MAC packets (excluding packets that were not good frames) received.
- **BeaconPkts—**Total beacon MAC packets detected by the probe.
- **ClaimPkts—**Total claim token MAC packets detected by the probe.
- **PurgePkts—**Total ring purge MAC packets detected by the probe.
- **Owner—**The entity that configured this entry.
- **DropEvnts**—Total number of times the ring enters a beaconing state

during this sampling interval.

Viewing Performance Statistics on the Segment

Double click on any instance (row or interface) in the Mac-Layer Statistics Table to view the RMON data presented in SPECTRUM Performance View format. This allows you to view current percentage calculations and a time graph of the interface activity, rather than the absolute numbers of the Statistics Table. Note that this view is dynamically updated.

Viewing Network Activity With the Multi-Attribute Line Graph

The Multi-Attribute Line Graph provides a general indication of network activity. The attributes' colors represent different statistics. Green represents Load, blue represents the Frame Rate, orange represents the error rate.

You can scroll back in time to view previously logged values for these attributes.

Use the graph properties button to modify the presentation of the graph. It has three options:

- Scroll to Date-Time—sets the viewing area to begin at a specified date and time.
- Change Time Scale—sets the Y axis time scale for the graph.
- Data Logging—data logging is not relevant for the Segment Performance Views of the RMON Probe models.

Use the Lin/Log toggle button to toggle between a linear and a logarithmic scale presentation of the graph.

Viewing Statistics with the Details Button

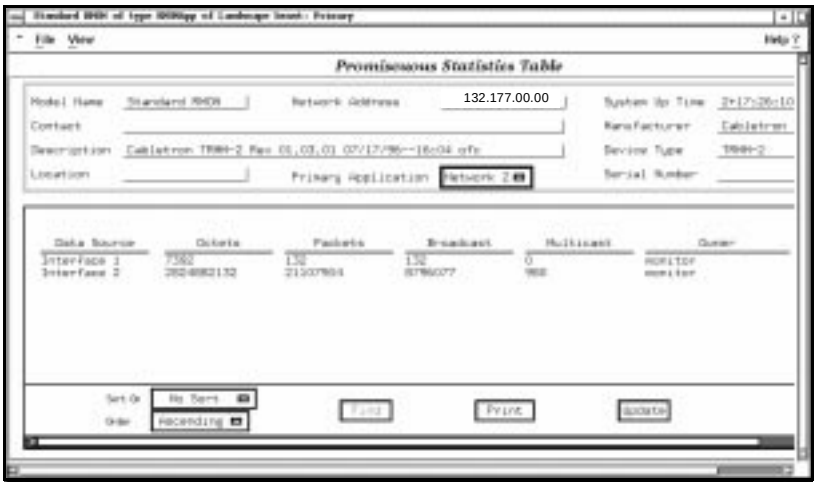
Click the Details button in the Performance View for more diagnostic detail. The Statistics Detail View appears; it presents a graphical breakdown of the isolating errors, non-isolating errors, and events. These statistics are updated and presented as totals or deltas. Each pie chart provides a color-coded view of events on the interface. Click on the Total, Delta, or Accum buttons to modify the data output.

- Total—The parameter's value over this instance's entire interval.
- Delta—The parameter's value over the duration of the update interval.
- Accum—The parameter's value over the interval since the Accum button was selected.

Promiscuous Statistics

From the Icon Subviews menu, click on Promiscuous Statistics. The Promiscuous Statistics Table (Figure 5-10) presents the RMON statistics in tabular form.

Figure 5-10. Promiscuous Statistics Table



The RMON Statistics group consists of the following 7 parameters measured at the monitored network interface (data source) of the device. These statistics take the form of free running counters that start from zero when a valid instance is created.

- **Data Source** —The interface being monitored.
- **Octets** —Total octets of data in packets collected promiscuously (excluding those that were not good frames) on the network.
- **Packets —**Total packets collected promiscuously (excluding packets that were not good frames).
- **Broadcast —**Total broadcast packets collected promiscuously by the probe.
- **Multicast —**Total multicast packets collected promiscuously by the probe.
- **Drop Events —**Total drop events detected by the probe.
- **Owner—**The entity that configured this entry.

Viewing Performance Statistics on the Segment

Double click on any instance (row or interface) in the Promiscuous Statistics Table to view the RMON data presented in SPECTRUM Performance View format. This allows you to view current percentage calculations and a time graph of the interface activity, rather than the absolute numbers of the Statistics Table. Note that this view is dynamically updated.

Viewing Network Activity With the Multi-Attribute Line Graph

The Multi-Attribute Line Graph provides a general indication of network activity. The attributes' colors represent different statistics. Green represents Load, blue the Frame Rate, orange the Broadcast and yellow the Multicast. You can scroll back in time to view previously logged values for these attributes.

Use the Lin/Log toggle button to toggle between a linear and a logarithmic scale presentation of the graph. Use the graph properties button to modify the presentation of the graph. It has three options:

- Scroll to Date-Time—sets the viewing area to begin at a specified and time.
- Change Time Scale—sets the Y axis time scale for the graph.
- Data Logging—data logging is not relevant for the Segment Performance Views of the RMON Probe models.

Viewing Statistics with the Frame Details Button

Click the Frame Details button in the Performance View for more diagnostic detail. This displays the Statistics Detail View which presents a graphical breakdown of the frame size distribution. These statistics are updated and presented as totals or deltas. Click on the Total, Delta, or Accum buttons to modify the data output.

- Total—The parameter's value over this instance's entire interval.
- Delta—The parameter's value over the duration of the update interval.
- Accum—The parameter's value over the interval since the Accum button was selected.

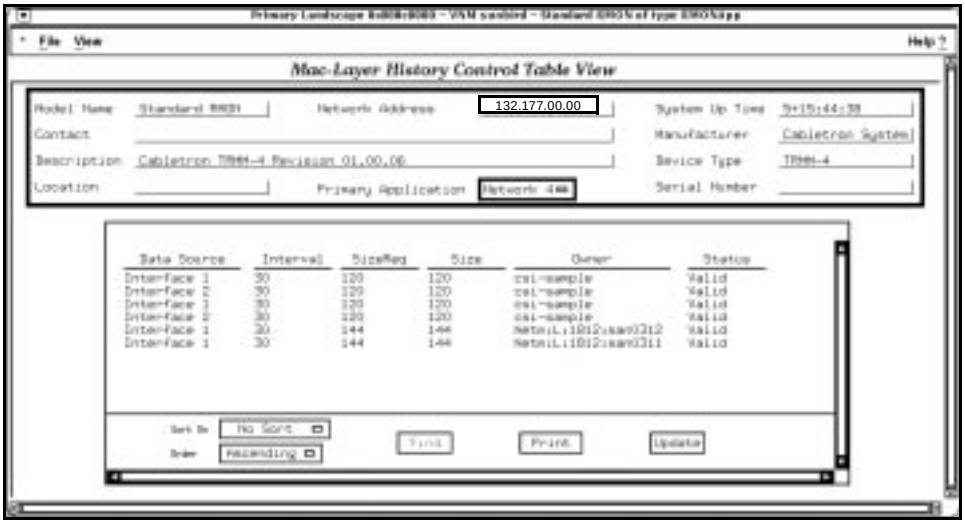
The Frame Breakdown pie chart provides a color coded view of the network segments total traffic by frame size, separated into the following catagories:

- 18 - 63
- 64 - 127
- 128 - 255
- 256 - 511
- 512 - 1023
- 1024 - 2047
- 2048 - 4095
- 4096 - 8191
- 8192 - 18000
- > 18000
- Total

Mac-Layer History

From the Icon Subviews menu, click on Mac-Layer History. The Mac-Layer History Table presents the RMON Mac-layer data in tabular form. The RMON History group records data from the Statistics group over user-defined intervals and stores it for later retrieval, allowing you to perform trend analysis of a statistic over time or to isolate periods of time during which a network event may have occurred.

Figure 5-11. Mac-Layer History Control Table View



The History Control Table (Figure 5-11) presents the configuration of each History instance running on the network interface. By default, the RMON standard specifies 2 instances, having intervals of 1800 seconds and 30 seconds. Each instance features the following fields:

- **Data Source**—Interface being monitored.
- **Interval**—The sample collection interval.
- **SizeReq**—Maximum number of recorded intervals (buckets) requested for the sample
- **Size**—The number of buckets correctly recorded in the sample.
- **Owner**—The person who configured the entry.
- **Status**—The status of the control table entry.

Note that when the values for SizeReq and Size are identical, the oldest entries in the History Control Table for that instance will be replaced by the newest entries.

Viewing the History Table

Double click any Mac-Layer History Control Table entry to display the data for that instance. The History Table shows the past performance measured at the monitored network interface (data source) of the device. Appendix B contains detailed descriptions of the fields found in the History Table.

Promiscuous History

From the Icon Subviews menu, click on Promiscuous History. ThePromiscuous History Table presents the RMON Promiscuous data in tabular form. The RMON History group records data from the Statistics group over user-defined intervals and stores it for later retrieval, allowing you to perform trend analysis of a statistic over time or to isolate periods of time during which a network event may have occurred.

Figure 5-12. Promiscuous History Control Table View

The History Control Table (Figure 5-12) presents the configuration of each History instance running on the network interface. By default, the RMON standard specifies 2 instances, having intervals of 1800 seconds and 30 seconds. Each instance features the following fields:

- **Data Source**—Interface being monitored.
- **Interval**—The sample collection interval.
- **SizeReq**—Maximum number of recorded intervals (buckets) requested for the sample
- **Size**—The number of buckets correctly recorded in the sample.
- **Owner**—The person who configured the entry.
- **Status**—The status of the control table entry.

Note that when the values for SizeReq and Size are identical, the oldest entries in the History Control Table for that instance will be replaced by the newest entries.

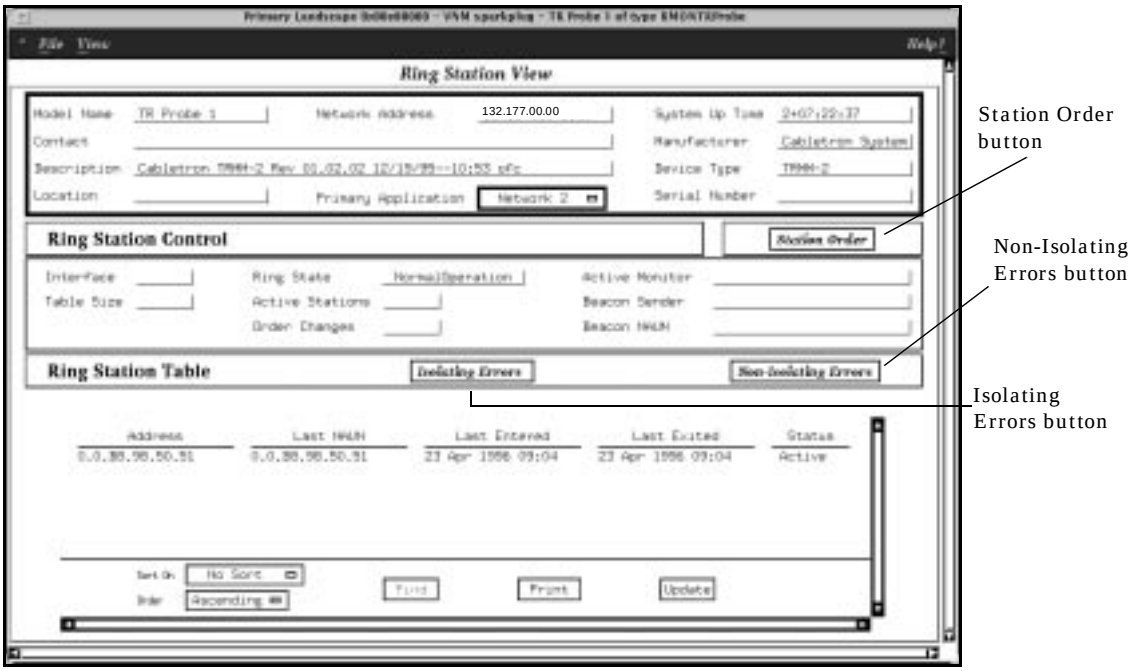
Viewing the History Table

Double click any Promiscuous History Control Table entry to display the data for that instance. The History Table shows the past performance measured at the monitored network interface (data source) of the device. Appendix B contains detailed descriptions of the fields found in the History Table.

Ring Station

From the Icon Subviews Menu, click on Ring Station. The menu selection is available only from the RMONTRProbe model. When you click on the Ring Station selection, the Ring Station Control View (Figure 5-13) appears. This Token Ring View includes the Ring Station and Ring Station Order Groups. The Ring Station group provides status information for the ring being monitored. In addition, it provides statistics and status information associated with each Token Ring station on the ring. The Ring Station Order group provides the order of the stations on the monitored ring.

Figure 5-13. Ring Station Control View

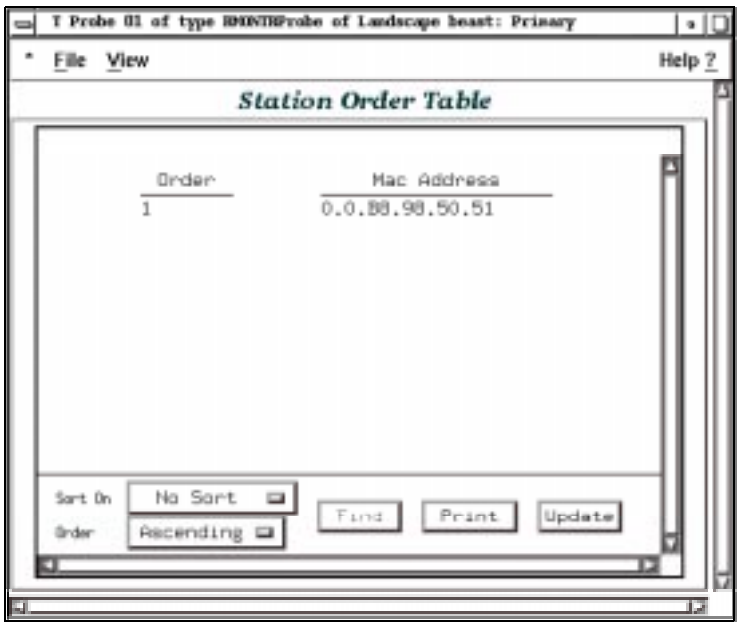


Appendix B contains detailed descriptions of the fields found in the Ring Station Control View.

Viewing the Station Order

Click on the Station Order button to view the Station Order Table which shows a screen similar to the following.

Figure 5-14. Station Order



The following fields appear in the Station Order Table.

Field	Description
Order	The location of this station with respect to other stations on the ring when the RMON probe gets the value one.
Mac Address	The physical address of this station.

Viewing Non-Isolating Errors

Click on the Non-Isolating Errors button to view data about non-isolating errors that occur on the network. Fields include:

- **Address**—The physical address of this station.
- **Token**—Total token errors reported in error reporting packets detected by the probe.
- **Duplicates**—The number of times the station experienced a duplicate address error.
- **Lost Frame**—Total lost frame errors reported in error reporting packets detected by the probe.
- **Copy Frame**—Total frame copied errors reported in error reporting packets detected by the probe.
- **Frequency**—Total frequency errors reported in error reporting packets detected by the probe.
- **Insertion**—Number of times the probe detected this station inserting onto the ring.
- **In Beacon**—Total number of beacon frames sent by this station and detected by the probe.
- **Out Beacon**—Total number of beacon frames detected by the probe that name this station as the NAUN.

Viewing Isolating Errors

Click on the Isolating Errors button to view data about isolating errors that the probe detects on the network. Fields include:

- **Address**—The physical address of this station.
- **In Line**—Total number of line errors reported by this station in error reporting packets.
- **Out Line**—Total number of line errors reported in error reporting packets sent by the nearest active downstream neighbor of this station.
- **In Burst**—Total number of burst errors reported by this station in error reporting packets.
- **Out Burst**—Total number of burst errors reported in error reporting packets sent by the nearest active downstream neighbor of this station.
- **A/C**—The total number of address copied errors reported in error reporting packets.
- **Abort**—The total number of abort delimiters reported in error reporting packets detected.
- **Internal**—The total number of adapter internal errors reported in error reporting packets.
- **Congestion**—The total number of receive congestion errors reported in error reporting packets.

Other RMON Views

All other RMON views that appear on Token Ring icons also appear on Ethernet icons. Refer to the preceding section on Ethernet Views for information on the following views:

- Hosts Control
- Matrix Control
- HostTopN Control

Accessing RMON Alarms/Events

The RMON Alarms/Events group monitors statistics, compares them to thresholds you set, and specifies the action that should be taken when a threshold is met. This subview selection is available only from the RMONApp model. Refer to Chapter 6, *Configuring RMON Alarms and Events*, for detailed information about how to create, modify, and delete RMON alarms and events.

Chapter 6

Configuring RMON Alarms and Events

This chapter describes the RMON Alarms and Events tables and how to create, modify, and delete RMON alarms and events.

RMON Alarms

An *alarm* is triggered when a *threshold* for a specified network activity, or *monitored object*, is crossed in a particular direction. You can set an alarm to be triggered when a monitored object goes above an indicated value (a *rising* threshold) or when it drops below an indicated value (a *falling* threshold).

You control what happens when an alarm is triggered. You map an alarm to an event, which can then generate a log entry on the agent or send a trap that is returned to your management station.

For example, you could set an alarm to be triggered when the agent detects a high level of Ethernet error packets on the network. When the alarm is triggered, an event sends a trap to your management station which, as detailed in the section on traps, can notify you through a SPECTRUM alarm or by other means such as phone, paging, trouble ticket, or electronic mail. In order to set meaningful thresholds for alarms, make sure you fully understand what is normal for your network.

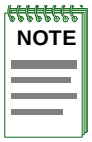
The RMON Alarms/Events View provides access to RMON Alarms and Events. This view is available only from the RMONApp model.

Click on the RMON Alarms/Events selection from the RMONApp's Icon Subviews menu. The Alarm/Event Table appears. Figure 6-1 shows the Alarms section of the RMON Alarm/Event Table View.

The following sections describe how to create an alarm, how to modify the characteristics of an existing alarm, and how to remove an alarm.

Creating an Alarm

Creating an alarm is a two-step process. The first step is to create an instance of a new alarm. The next step is to make the alarm Valid, thus enabling the alarm.



In the configuration views for RMON Alarms and Events, some attribute fields are outlined in red. This is normal; it occurs when you define a new alarm or event because a value for the attribute does not yet exist. After you enter a value, the attribute outline changes to white.

To create an alarm, follow these steps:

1. Click on the RMON Alarms/Events selection from the RMONApp's Icon Subviews menu. The Alarm/Event Table View appears. Adjust the vertical slide bar to see the Alarm Table (shown below).
2. Click on the New Alarm button. The Alarm Creation View appears.

Figure 6-1. Alarm Table and Alarm Creation View

3. In the Owner field, enter the name of the alarm's owner.
4. Click in the Index field and enter a number that represents this alarm definition. Make sure the Index number you choose is not already assigned to an existing alarm definition. The alarm indexes in use need not be consecutively numbered.

5. Click on the Status button and select **createRequest** from the Status menu.

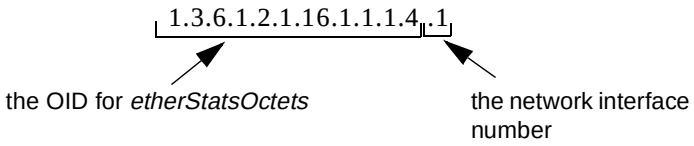
6. Click on the Start-up Alarm button and select the type of threshold that will trigger this alarm. Threshold types are:

   - **Rising**—The value for the monitored object rises above the threshold
   - **Falling**—The value for the monitored object falls below the threshold
   - **Rising_or_Falling**—The value for the monitored object rises above or falls below the threshold

7. Click in the Variable field and enter the object ID (OID) you want to monitor. (You can monitor any OID in the SNMP MIB of the device.) See Appendix B for a listing and description of RMON objects and OIDs.

   (An OID is a numerical representation of an RMON object. If you are unfamiliar with OIDs, see RFCs 1271 and 1513 for information about Ethernet and Token Ring objects and OIDs.)

   When you enter an OID, you must append the number of the interface (on which the object will be monitored) to the object's OID. For example, assume that you modeled an EMME that has four interfaces and you want to create an alarm for the object *etherStatsOctets* on interface 1. To monitor the object on network interface 1, you would enter the OID in the following format:



8. In the Threshold Information box, click in the Falling Threshold field and enter the low threshold for the sampled statistic. A single alarm is generated for the object if either of the following conditions is met:

   - The current sampled value is less than or equal to this threshold, and the current value at the last sampling interval was greater than this threshold.
   - The first sample taken after this entry became valid is less than or equal to this threshold, and the associated Startup Alarm is equal to Falling or Rising_or_Falling.

   After a falling alarm is generated, a second one is not generated until the sampled value rises above the Falling Threshold and reaches the Rising Threshold.

9. Click in the Falling Event Index field and enter the index of the Falling Threshold Event definition. This is the event in the Event Table which will be generated when this Falling Threshold Alarm is triggered. Use this

to control the type of notification you want. See the steps outlined in *RMON Events*.

10. Click in the Rising Threshold field and enter the high threshold for the sampled statistic. A single alarm is generated for the object if either of the following conditions is met:

    - The current sampled value is greater than or equal to this threshold and the value at the last sampling interval was less than this threshold.
    - The first sample after this entry becomes valid is greater than or equal to this threshold and the associated Startup Alarm is equal to Rising_or_Falling or Rising.

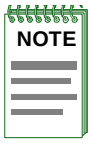
    After a rising alarm is generated, another rising alarm will not be generated until the sampled value falls below the Rising Threshold and reaches the Falling Threshold.

11. Click in the Rising Event Index field and enter the index of the Rising Threshold Event definition. This is the event in the Event Table which will be generated when this Rising Threshold Alarm is triggered. Use this to control the type of notification you want. See the steps outlined in *RMON Events*.

12. Enter the Rate and Sample Type in the Sampling Information box.

    - Rate—The interval in seconds over which data is sampled and compared with the rising and falling thresholds.
    - Sample Type—The method of sampling the selected variable. Choices are:
        - **Absolute**—The value of the selected variable is compared directly with the thresholds at the end of the sampling interval.
        - **Delta**—The value of the selected variable at the last sample is subtracted from the current value and the difference compared with the thresholds.

13. To complete the process, click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears. At this point you should see the Status button change to underCreation.



If you want to modify your selections, you can reenter the information as long as the Status button indicates the alarm is underCreation. Do not modify your entry for the Index field in an attempt to create another alarm. Close the window and select New Alarm if you want to create another alarm.

14. Close the window and return to the Alarm Table View.

15. To see the alarm instance you created, click Update in the Alarm Table. The new alarm definition appears in the table, the Status field reads **underCreation,** and the alarm's values appear.

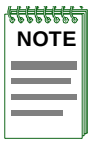
Now that you have created the alarm, you must change the alarm's status to Valid. Note that Cabletron RMON agents on the device will delete an alarm whose status remains underCreation for an extended period of time. (RMON agents produced by other companies might not delete alarms that are under creation.)

To change the alarm's status, follow the steps outlined in the following section, *Modifying and Enabling an Alarm Under Creation*.

Modifying and Enabling an Alarm Under Creation

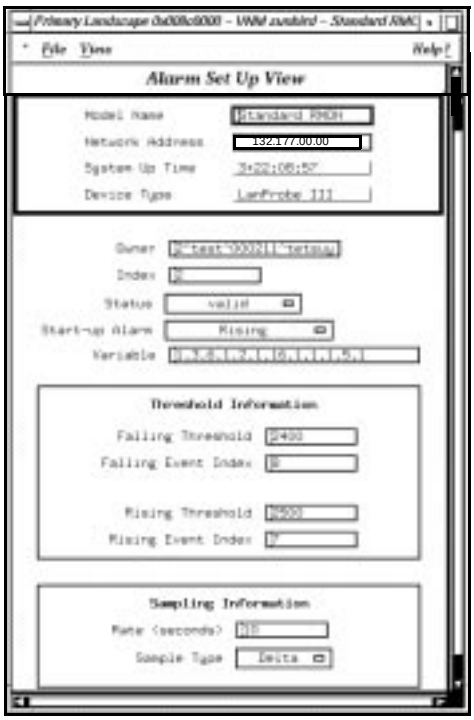
Follow these steps to modify and enable an alarm:

1. In the Alarm Table, double click on the alarm's entry. The Alarm Set Up View appears.



Do not modify the Index field in an attempt to modify another alarm. To configure a different alarm, close the window and select the other alarm.

Figure 6-2. Alarm Set Up View



2. You can modify the following fields. For a description of these fields see the previous section, *Creating an Alarm*.

   - Owner
   - Start-up Alarm
   - Variable
   - Threshold Information
   - Sampling Information

3. To enable the alarm, click on the Status button (located above the Description Information box) and select **valid**. Remember that Cabletron's RMON agent will delete the alarm if you neglect to change the status to valid.

4. To complete the process, click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears. Close the window and return to the Alarm Table View.

5. Dismiss the Alarm Set Up View window.

6. To see the new configuration, click Update in the Alarm Table. The Status field now reads **valid** and the alarm's values are shown.

Modifying a Valid Alarm

To modify an alarm that is in the valid state, you must first return the alarm to the underCreation state. After making your changes, return the Alarm to the valid state.

To modify an existing alarm definition in the Alarm Table, follow these steps:

1. Double click on the alarm entry you want to change. The Alarm Setup View appears.

2. Click on the Status button and select underCreation from the menu.

3. Click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears. The alarm is placed in the underCreation state. To verify this, select Update in the Alarm View and observe the state change in the Alarm Table.

4. Follow the steps outlined in the previous section, *Modifying and Enabling an Alarm Under Creation*.

Removing an Alarm

To remove an alarm from the table, follow these steps:

1. Double click on the alarm in the Alarm Table to access the Alarm Set Up View.
2. Click on the Status button and select invalid from the menu.
3. Click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears. The alarm will now be removed from the Alarm Table. Dismiss the Alarm Set Up View window.
4. Click on Update in the Alarm Table to verify that the alarm was removed.

RMON Events

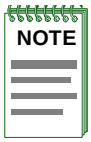
Click on the RMON Alarms/Events selection from the RMONApp's Icon Subviews menu. The Alarm/Event Table appears. Figure 6-3 shows the Events section of the RMON Alarm/Event view.

When you define an event, you specify the action that the RMON agent should perform when a specified network activity occurs. By default, RMON on the device configures three events: High Threshold Exceeded, Low Threshold Exceeded, and Packet Match Occurrence.

The following sections describe how to create an event, modify an existing event, view the event log, and remove an event.

Creating an Event

Creating an event is a two-step process. The first step is to create an instance of a new event. The next step is to make the event valid, thus enabling the event.

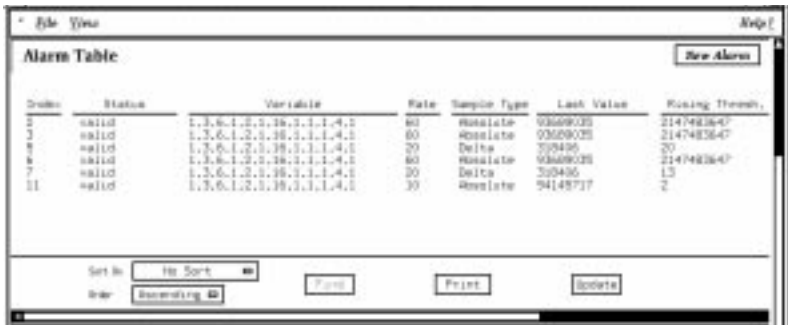


In the configuration views for RMON Alarms and Events, some attribute fields are outlined in red. This is normal; it occurs when you define a new alarm or event because a value for the attribute does not yet exist. After you enter a value, the attribute outline changes to white.

To create an event, access the Event Set UpView, where you supply values for the parameters that define the event. Follow these steps:

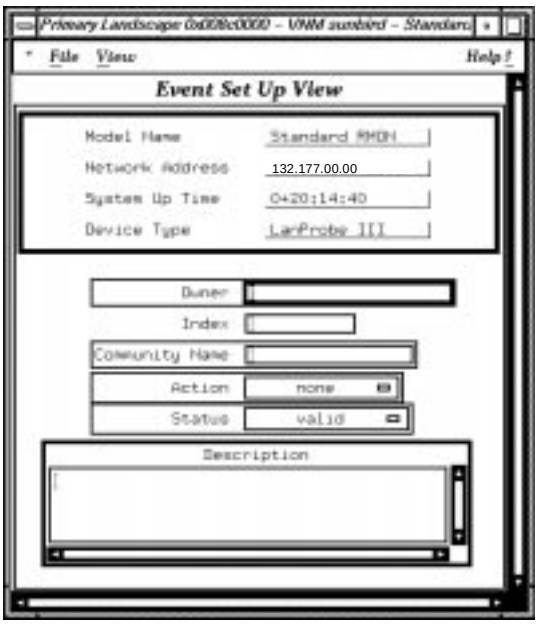
1. Click on RMON Alarms/Events in the RMONApp's Icon Subviews menu. The Alarm/Event Table View appears. Adjust the vertical slide bar to see the Event Table (shown in Figure 6-3).

Figure 6-3. Event Table View



2. In the Event Table, click on the New Event button to access the Event Set Up View, shown in Figure 6-4.

Figure 6-4. Event Set Up View



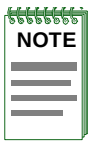
3. In the Owner field, enter the name of the event's owner.

4. In the Index field, enter a number that represents this event definition. Make sure the Index number you choose is not already assigned to an existing event definition. The event indexes in use need not be consecutively numbered.

5. Click in the Community Name field and enter a text string that identifies the SNMP community to which an SNMP trap will be sent. See the section entitled *Traps* for details.

6. Click on the Action button and select the action required in response to an alarm.

   - **none**—Make no notification of the event
   - **log**—Record the event in the log table
   - **snmp-trap**—Send an SNMP trap to one or more management stations
   - **log-and-trap**—Record the event in the log table and send an SNMP trap to one or more management stations

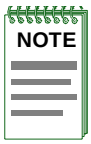


In order to use traps, you must have a network management environment (such as SPECTRUM) that supports them. In addition, trap destination information must be configured for the agent. See the section entitled "Traps" for details.

7. Click in the Description field and enter a text string that describes the event. This description will be included in this event's entries in the Event Log View and Trap messages.

8. Click on the Status button and select **createRequest** from the Status menu.

9. To complete the process, click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears. At this point, you should see the Status button change to underCreation.



If you want to modify your selections, you can reenter the information as long as the Status button indicates the event is underCreation. Do not modify your entry for the Index field in an attempt to create another event. Close the window and select New Event if you want to create another event.

10. Close the Event Set Up View and return to the Event Table View. To see the new event instance you created, the Event Table View must be updated to reflect the new configuration. Click Update in the Event Table. The new event's default values appear in the Event Table and the Status field reads **underCreation**.

Now that you have created the event, you must change the status to valid. Note that Cabletron RMON agents on the device will delete an event whose status remains underCreation for an extended period of time. (RMON agents produced by other companies might not delete events that are under creation.) To change the status of the new event to valid, follow the steps outlined in *Modifying and Enabling an Event underCreation*.

Modifying and Enabling an Event Under Creation

1. In the Event Table, double click on the event's entry. The Event Set Up View appears.
2. You can modify the following fields. For a description of these fields, see the previous section, *Creating an Event*.
   - Owner
   - Community Name
   - Action
   - Description
3. To enable the event, click on the Status button (located above the Description Information box) and select **valid**. Remember that Cabletron's RMON agent will delete the event if you neglect to change the status to valid.
4. To complete the process, click the right mouse button, or select Save All Changes from the File menu, and click OK in the Save Changes dialog box that appears. Close the window and return to the Event Table View.
5. To see the new configuration, the Event Table View must be updated to reflect the new configuration. Click Update in the Event Table. The Status field now reads **valid** and the event's values are shown.

Modifying a Valid Event

To modify an event which is in the valid state, you must first return the event to the underCreation state. After making your changes, return the Event to the valid state.

To modify an existing event definition in the Event Table, follow these steps:

1. Double click on the event entry you want to change. The Event Setup View appears.
2. Click on the Status button and select underCreation.
3. Click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears. The event will now be placed in the underCreation state. To verify this, select Update in the Event View and observe the state change in the Event Table.
4. Follow the steps outlined in the previous section, *Modifying and Enabling an Event Under Creation*.

Removing an Event

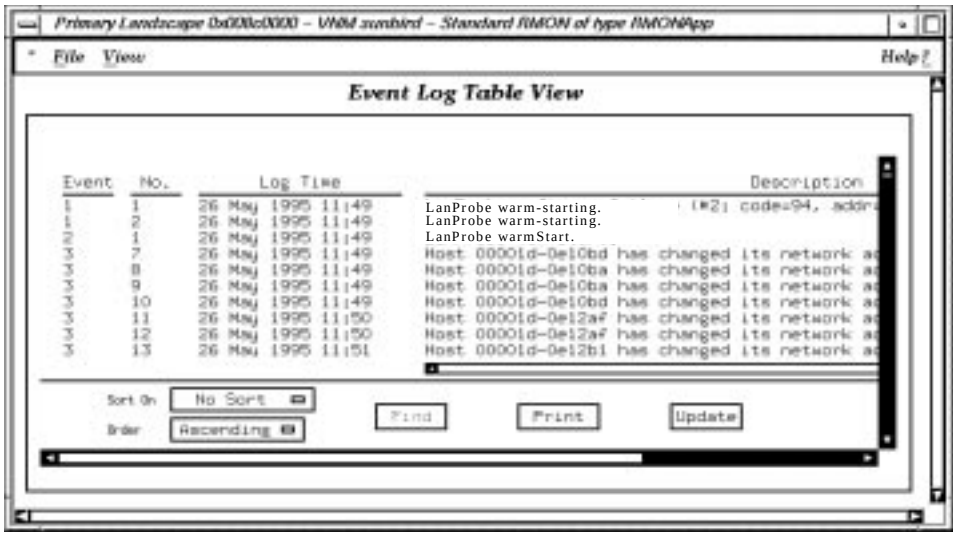
To remove an event from the table, follow these steps:

1. Double click on the event in the Event Table to access the Event Set Up View.
2. Click on the Status button and select **invalid** from the Status menu.
3. Click the right mouse button, or select Save All Changes from the File menu, and click OK in the dialog box that appears. The event will now be removed from the Event Table. Dismiss the Event Set Up View window.
4. Click on Update in the Event Table to verify the event was removed.
5. A dialog box informs you that the event no longer exists. Click on OK.

Viewing the Event Log

In the Event Table, click on the View Event Log button to view the Event Log Table, which contains detailed descriptions of all recorded events.

Figure 6-5. Event Log Table View


File View
Help ?
Event Log Table View
Event No. Log Time Description
1 1 26 May 1995 11:49 LanProbe warm-starting.
1 2 26 May 1995 11:49 LanProbe warm-starting.
2 1 26 May 1995 11:49 LanProbe warmStart.
3 7 26 May 1995 11:49 Host 00001d-0e10bd has changed its network ad
3 8 26 May 1995 11:49 Host 00001d-0e10ba has changed its network ad
3 9 26 May 1995 11:49 Host 00001d-0e10ba has changed its network ad
3 10 26 May 1995 11:49 Host 00001d-0e10bd has changed its network ad
3 11 26 May 1995 11:50 Host 00001d-0e12af has changed its network ad
3 12 26 May 1995 11:50 Host 00001d-0e12af has changed its network ad
3 13 26 May 1995 11:51 Host 00001d-0e12b1 has changed its network ad
Sort On No Sort
Order Ascending
Find
Print
Update

The following fields appear in the Event Log Table:

- **Event**—The index number of the event which was logged.
- **No.**—Entry sequence per defined event (index number).
- **Log Time**—The value of sysUpTime when this log entry was created.
- **Description**—A text string describing the alarm which triggered this event.

Traps

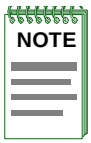
When you define an event on the RMON agent, you can specify the action to be taken when the event occurs. The event can be recorded in a log on the RMON agent, it can generate an SNMP trap for notification at your management station, or both.

With traps, the management station doesn't need to continuously poll the agent for information about network conditions. Instead, the burden is on the agent to monitor the network and notify the management station when a notable event occurs.

If you plan to define RMON events which will send SNMP traps, you must first configure both the RMON agent and your management station to handle them. This section describes that process.

SPMA Trap Table Tool

The SPECTRUM Portable Management Application Trap Table Tool is part of the SPMA Tools which are available from Cabletron as part of the SPMA core product. This tool is not needed to perform the steps when you configure traps; however, its use will simplify trap table configuration. Where appropriate, this tool is referred to in the following section.

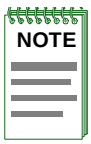


Traps are an SNMP facility that acts on behalf of the RMON agent or other function on a device. This facility is not part of the RMON standard itself.

Management Station

Typically, traps received by a management station are saved as entries in event logs on the management station. With SPECTRUM, you will see these traps as events in SPECTRUM's Event Log and no configuration is necessary to accomplish this.

Also, these events are integrated with SPECTRUM's Alarm View so you are alerted by a SPECTRUM alarm when they occur. If you choose, you can use SPECTRUM Applications such as SpectroPhone, Remedy Gateway or the SPECTRUM Alarm Notifier to extend the notification to include paging, phone notification, trouble ticketing, electronic mail, and so on.



While configuring events to generate traps, you will encounter an event community name parameter, sometimes referred to as a trap destination group. This identifies a group of trap destinations defined at the RMON agent. This is not the community name of the destination management station.

RMON Agent

When an SNMP device on the network generates a trap as a result of some condition on that device, the device must know where to send the trap (the trap destination). For Cabletron devices such as an EMME, there is a Trap Destination Table which is user-configurable and accessed through local management via the front panel console port on the EMME or remotely with the SPMA Trap Table Tool.

If you are not using Cabletron devices or agents, be aware that trap destination tables are not yet part of the SNMP standard, so many vendors implement a proprietary method for specifying trap destinations. Consult the documentation of your RMON probe or agent for information on configuring trap destinations and for compatibility with this application.

The following instructions for configuring the Trap Table apply to all Cabletron Devices, since the local management is the same or very similar. When you configure the trap table, you can use either of the following methods.

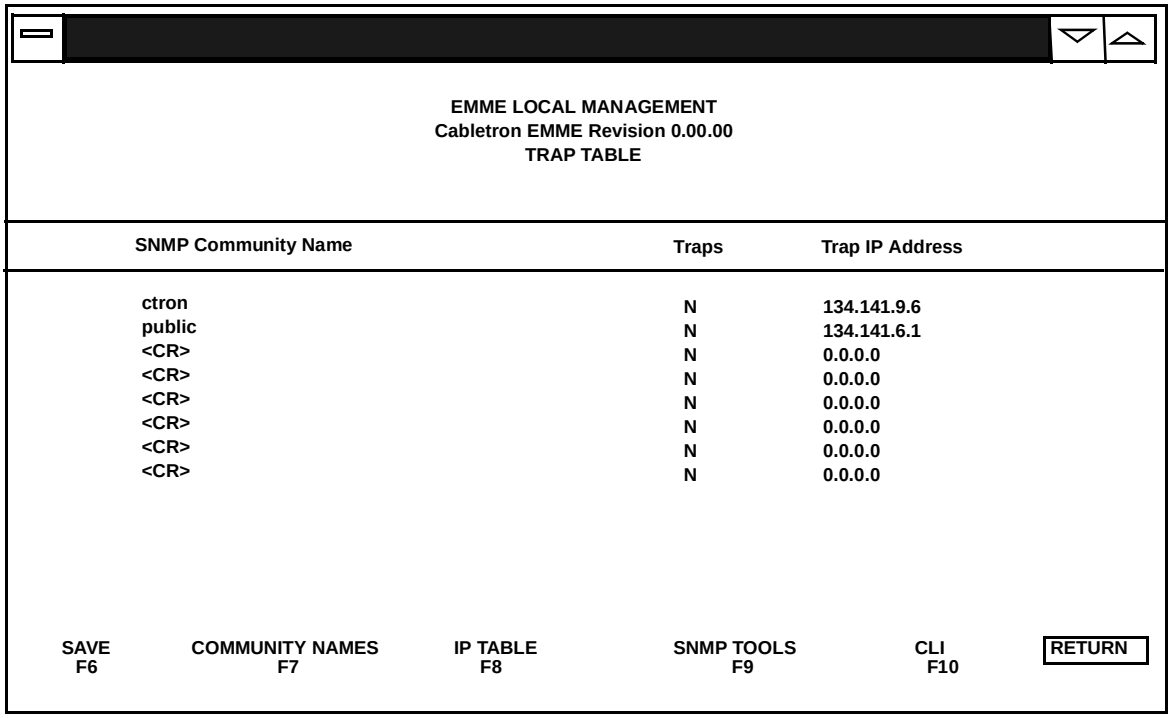
The SPMA Trap Table Tool—This tool provides remote configuration of Cabletron device Trap Tables. If you choose to use this tool please refer to the SPMA Tools User Guide for instructions.

Local Management—The Trap Destination Table is accessed through local management via the front panel console port on the device. The documentation for your particular device contains all the necessary instructions regarding equipment and procedures for using local management. The following instructions pertain to configuring the Trap Destination Table only. If you need further information regarding local management please refer to the user manual which accompanied your device.

Accessing the Trap Table Screen

To access the Trap Table Screen from the Features Selection Screen, use the arrow keys to highlight the Component Trap Table option and press the Return key (or F8). The Trap Table Screen, shown in Figure 6-6, appears.

Figure 6-6. Trap Table Screen



The Trap Table Screen contains the following fields:

- **SNMP Community Name**—The community name serves two purposes. First, it is a Trap IP Address identifier, which uniquely identifies the particular Trap IP Address it is associated with in the table, or a number of Trap IP Addresses if the same identifier is applied to more than one address. Its purpose is to define subsets of addresses in the table to send traps to, depending on the event community name in the trap request coming from the function on the device. A trap is sent only to those Trap IP Addresses (management stations) whose community name in the Trap Table matches the community name in the request. This allows you to send a trap only to those management stations which would be interested in that information. In this case, the trap request is coming from the RMON agent.

Note that this is not a community name of the destination management station itself, which typically is not a factor in receiving traps. However, this event community name is embedded in the trap message and can be accessed by applications at the destination to allow an application to decide whether the trap is of interest. This is the second purpose of the community name in the Trap Destination Table, and currently neither SPECTRUM nor any of its applications make use of it.

- **Traps**—Enables transmission of the traps to the network management station with the associated IP Address.
- **Trap IP Address**—The IP Address of the workstation that will receive trap alarms.

Configuring the Trap Table

1. Use the arrow keys to highlight the SNMP Community Name field and enter the community name. Press Return.
2. Use the arrow keys to highlight the Traps field and enter **Y** to send alarms to the workstation, or **N** to prevent alarms from being sent. Press Return.
3. Use the arrow keys to highlight the appropriate Trap IP Address field.
4. Enter the IP Address of the workstation to send traps using this field. Use the XXX.XXX.XXX.XXX format with the value of XXX ranging from 0 to 255.
5. Use the arrow keys to highlight the SAVE option and press Return (or press F6). The message SAVED OK will appear on the screen.

   If you exit without saving, you will lose your edits.
6. To exit the screen, press the appropriate Function key, or use the arrow keys to highlight RETURN and press the Return key. The latter exits you to the Feature Selection Screen.

Chapter 7

Creating IndirectRMON Models

This chapter describes how to set up IndirectRMON models.

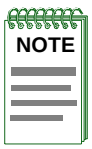
IndirectRMON Models

The IndirectRMON Model Type was designed to take advantage of additional network monitoring possibilities made available by data contained in the Host Table.

A number of hosts on the network, whose MAC addresses are in the Host Table, may not be using SNMP as a management protocol or otherwise may not be supported by SPECTRUM, yet their traffic statistics are visible to RMON. The IndirectRMON model, which you can create, accesses the RMON Host Table to acquire these management statistics which are not available in the normal fashion of polling. Therefore, this model provides a means to present status and performance statistics for such devices in the normal fashion of a SPECTRUM model.

This model offers another advantage in that it provides current performance statistics on any host without the need to access the RMON Host Table.

Also, by modeling the device by MAC address only, the modeling method provides the convenience of not having to locate or identify the actual device type and IP address. In fact, the device may not even have an IP address.



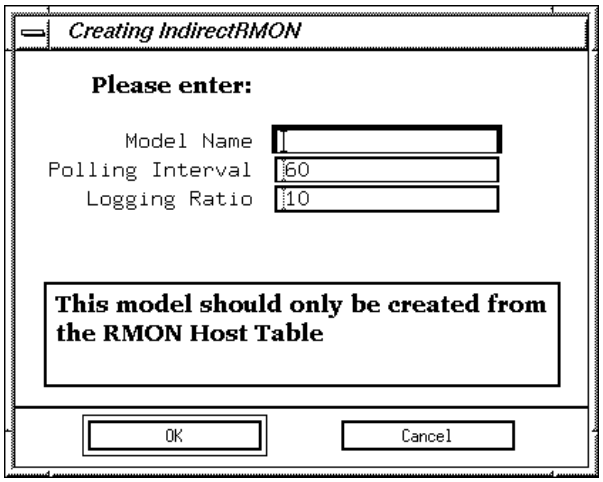
Before you use the IndirectRMON Model Type, consider using the Generic SNMP Device model type (GnSNMPDev) provided by SPECTRUM for modeling any SNMP capable device for which a specific model type is unavailable. To use GnSNMPDev, however, you must know the device's IP address.

Creating an IndirectRMON Model

You create an IndirectRMON model from within the RMON Host Table View. To create an IndirectRMON model, follow these steps:

1. Select the Hosts Control menu item from the Icon Subviews menu.
2. Double click on an instance within the Host Control Table. The Host Table View appears.
3. In the Host Table, choose the device you want to model and double click on the row containing the chosen MAC address. The Host Table Detail view appears.
4. Click on the Create Indirect Model button. A red Select Model Type dialog box appears.
5. Select the IndirectRMON model type in the dialog box, if it is not already highlighted.
6. Click OK. The IndirectRMON Creation View (Figure 7-1) appears.

Figure 7-1. IndirectRMON Creation View



7. In the Model Name field, assign a unique Model Name to identify the model of the device.
8. Accept the default Polling Interval (60 seconds) or click in the Polling Interval field and supply a different value.
9. Accept the default Logging Ratio (10) or click in the Logging Ratio field and supply a different value.

10. Click OK to create the model.

The IndirectRMON Creation View disappears and the newly created IndirectRMON model icon is placed into the Lost & Found view. The following section describes how to move the Indirect RMON icon from the Lost & Found view to its proper location in a LAN segment.

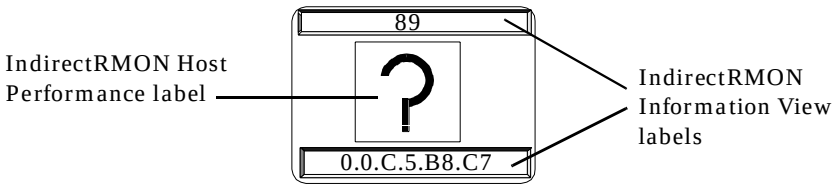
Placing an IndirectRMON Model into a View

To place an IndirectRMON model into a SPECTRUM view, follow these steps:

1. From SPECTRUM's View menu, select New View Lost & Found.
2. Place the Lost + Found view into Edit mode and select the IndirectRMON model.
3. Select Copy from the Edit menu to place the model into a paste buffer. Click OK on the buffer overwrite prompt.
4. Select Save & Close from the File menu or click the right mouse button to close out of the edit function.
5. Navigate into a Topology view of the LAN model into which you want to place the IndirectRMON model.
6. Select Edit from SPECTRUM's File menu.
7. Select Paste from the Edit menu to place the IndirectRMON model in the view. Wait for the icon to paint fully on the screen and then drag the icon to the desired position in the view.
8. Select Save & Close from the File menu to close out of the edit function.

The IndirectRMON Icon

Figure 7-2. IndirectRMON Icon



The IndirectRMON icon features three labels that provide visual status and quick access to detailed information about the model:

- The IndirectRMON Information View label (at the top of the icon) displays the default or user-defined model name.
- The IndirectRMON Information View label (at the bottom of the icon) displays the MAC address of the device
- The IndirectRMON Host Performance label (in the center of the icon) provides a representative image of the IndirectRMON model type, as well as visual status.

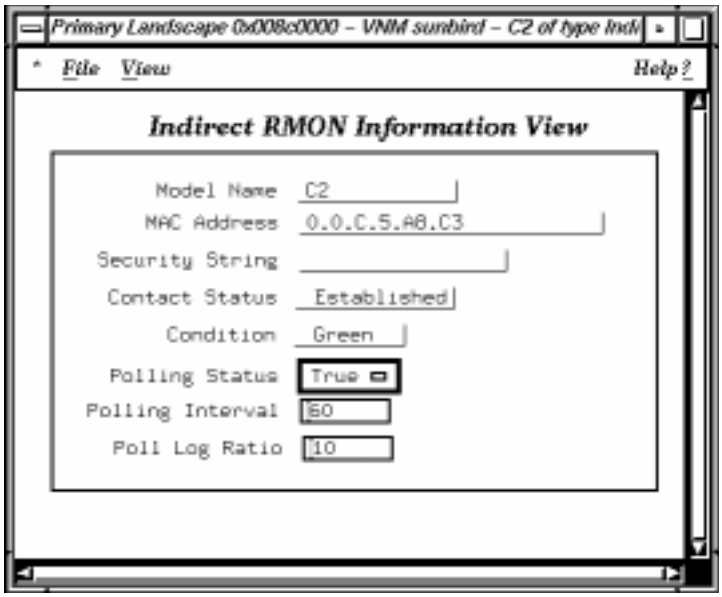
To access the information, double click on the label, using the left mouse button. You can also access this same information through the Icon Subviews menu. The next sections describe the views that appear when you double click on these labels.

These views, along with others associated with the Off-Page Reference icon, can also be accessed through the Icon Subviews menu of the View menu.

IndirectRMON Information View Label

Double click on the IndirectRMON icon's Information View label to open the IndirectRMON Information View (Figure 7-3).

Figure 7-3. IndirectRMON Information View



The following fields appear in the Information View:

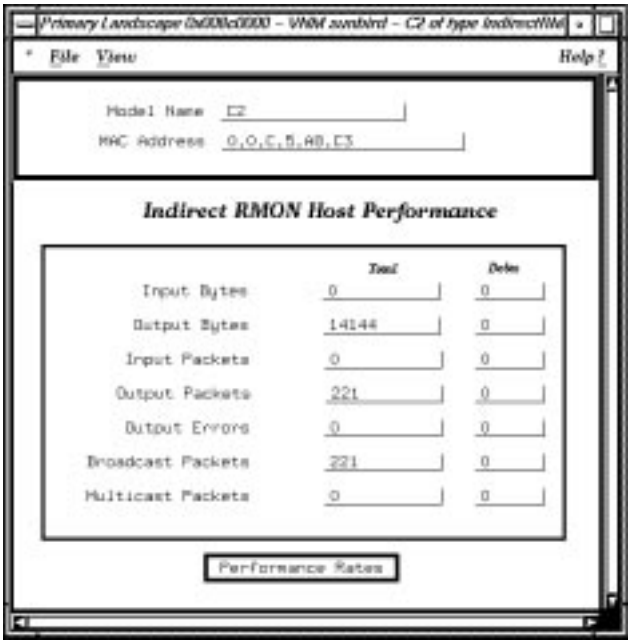
- **Model Name**—The model name for the IndirectRMON model.
- **MAC Address**—The MAC address for the IndirectRMON model.
- **Security String**—The user-assigned security string for the IndirectRMON model.
- **Contact Status**—The contact status of the IndirectRMON model. Possible values are Established, Lost, or Initial.
- **Condition**—The status of the IndirectRMON model. Possible values are blue, green, red, and gray.
- **Polling Status**—The current polling status of the IndirectRMON model.
- **Polling Interval**—The time interval in seconds during which SpectroSERVER reads all attributes of the IndirectRMON model that are flagged as POLLED.
- **Poll Log Ratio**—The number of SpectroSERVER polls of an IndirectRMON model that occur prior to logging the poll results in the database.

IndirectRMON Host Performance Label

The IndirectRMON icon's Host Performance label provides a representative image of the IndirectRMON model type, as well as visual contact status.

Double click on the question mark in the center of the icon to access the IndirectRMON Host Performance view (Figure 7-4). This view contains traffic data attributes for the host modeled by the IndirectRMON model. The data dynamically changes to reflect total and delta performance statistics for the IndirectRMON model.

Figure 7-4. IndirectRMON Host Performance Information



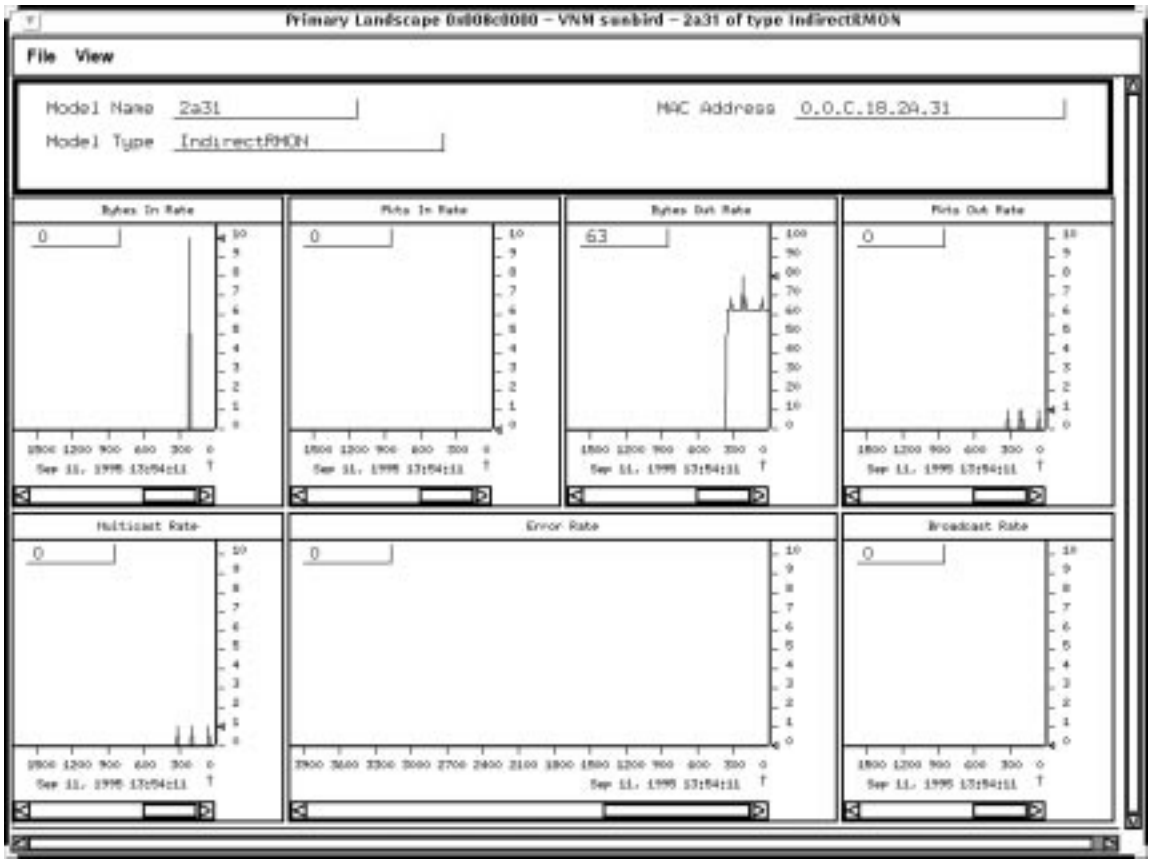
In addition to the Model Name and the MAC Address, the following fields appear in the Host Performance view:

- **Input Bytes**—The number of octets transmitted to this address since it was added to the Host Table, excluding those octets in packets that contained errors.
- **Output Bytes**—The number of octets transmitted by this address since it was added to the Host Table, including those octets in packets that contained errors.
- **Input Packets**—The number of packets without errors transmitted to this address since it was added to the Host Table.
- **Output Packets**—The number of packets including errors transmitted by this address since it was added to the Host Table.
- **Output Errors**—The number of error packets transmitted by this address since this host was added to the Host Table.

- **Broadcast Packets**—The total number of good packets transmitted by this address that were directed to the broadcast address since this host was added to the Host Table.
- **Multicast Packets**—The total number of good packets transmitted by this address that were directed to a local or global multicast or functional address since this host was added to the Host Table.

Click on the Performance Rates button to view each traffic data attribute in graphical format, as shown in Figure 7-5.

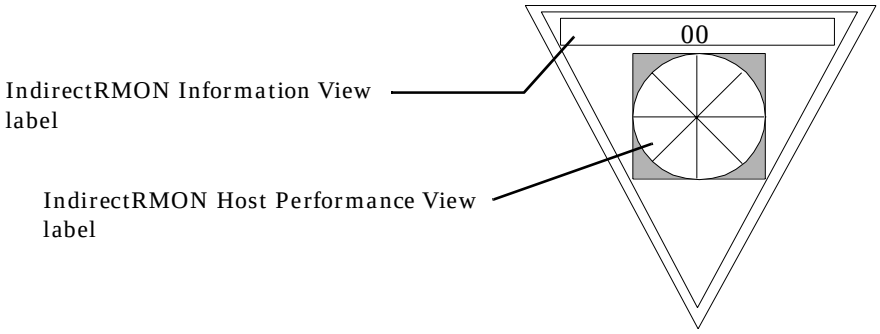
Figure 7-5. Performance Rates



The Off-Page Reference Icon

The Off-Page Reference Icon (Figure 7-6) represents a device that is directly connected to the current level of view but which was modeled from another view. The icon features two areas (the IndirectRMON Information View label and the IndirectRMON Host Performance View label) that you can double click to access informational views about the device. These views, along with others associated with the Off-Page Reference icon, can also be accessed through the Icon Subviews menu of the View menu.

Figure 7-6. Off-Page Reference Icon



IndirectRMON Information View Label

Double click on the IndirectRMON Information View label (which displays the user-defined model name) to view configuration information about the device.

IndirectRMON Host Performance View Label

The IndirectRMON Host Performance View label color reflects the device's contact status.

Appendix A

Ethernet Fields and Statistics

This appendix describes the Ethernet fields and statistics that appear in the RMON Management Module views.

Ethernet Statistics Table

Listed below is a description of the fields found on the Ethernet Statistics Table.

Field	Description
Data Source	The source of the data that this entry is configured to analyze. The source can be any Ethernet interface on this device.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including error packets) received.
Broadcasts	The total number of good packets received that were directed to the broadcast address.
Multicasts	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Owner	The entity that configured this entry and is therefore using the resources assigned to it.
CRC/Align	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).

Field	Description
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Fragments	The total number of packets received that were not an integral number of octets in length or that had a bad FCS, and were less than 64 octets in length (excluding framing bits but including FCS octets).
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and were not an integral number of octets in length or had a bad FCS.
Oversized	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Undersized	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Drop Events	The total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is the number of times this condition has been detected.

Ethernet Statistics Detail View

This section describes the fields found in the Frame Breakdown and Error Breakdown charts.

Frame Breakdown Chart

The following fields appear in the Frame Breakdown chart. Values in all of the fields include Frame Check Sequence octets but exclude framing bits.

Field	Description
Undersize	The total number of packets received that were less than 64 octets long and were otherwise well-formed.

Field	Description
64 Bytes	The total number of packets, including error packets, that were 64 bytes in length.
65 to 127 Bytes	The total number of packets, including error packets, that were between 65 and 127 bytes in length inclusive.
128 to 255 Bytes	The total number of packets, including error packets, that were between 128 and 255 bytes in length inclusive.
256 to 511 Bytes	The total number of packets, including error packets, that were between 256 and 511 bytes in length inclusive.
512 to 1023 Bytes	The total number of packets, including error packets, that were between 512 and 1023 bytes in length inclusive.
1024 to 1518 Bytes	The total number of packets, including error packets, that were between 1024 and 1518 bytes in length inclusive.
Oversized	The total number of packets received that were longer than 1518 octets and were otherwise well-formed.
Total	The total number of packets received.

Error Breakdown Chart

The following fields appear in the Error Breakdown chart. Values in the Alignment, Fragments, and Jabbers fields include Frame Check Sequence octets but exclude framing bits.

Field	Description
Alignment	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Fragments	The total number of packets received that were not an integral number of octets in length or that had a bad FCS, and were less than 64 octets in length (excluding framing bits but including FCS octets).

Field	Description
Jabbers	The total number of packets received that were longer than 1518 bytes and were not an integral number of octets in length or had a bad Frame Check Sequence.
Total	The total number of packets received.

Ethernet History Control Table

The following fields appear in the Ethernet History Control Table.

Field	Description
Data Source	The source of the data for which historical data was collected and placed in a media-specific table on behalf of this entry. The source can be any interface on the device.
Interval	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this history control entry.
SizeReq	The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.
Size	The number of discrete sampling intervals over which data has been saved in the part of the media-specific table associated with this entry.
Owner	The entity that configured this entry and is using the resources assigned to it.
Status	The status of this entry.

History Table

The following fields appear in the History Table.

Field	Description
Created	The value of sysUpTime at the start of the interval over which this sample was measured. If the probe keeps track of the time of day, it starts the first sample when the next hour of the day begins.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this interval in hundredths of a percent.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence octets).
Packets	The number of packets (including error packets) received during this sampling interval.
Broadcasts	The number of good packets received during this sampling interval that were directed to the broadcast address.
Multicasts	The number of good packets received during this sampling interval that were directed to a multicast address.
Collisions	The best estimate of the number of collisions on this Ethernet segment during this interval.
CRC Errors	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but were not an integral number of octets in length or had a bad FCS.
Undersized	The number of packets received during this interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well-formed.
Oversized	The number of packets received during this interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Drop Events	The total number of events in which packets were dropped by the probe due to lack of resources during this interval.
Fragments	The total number of packets received during this sampling interval that were not an integral number of octets in length or that had a bad FCS, and were less than 64 octets in length (excluding framing bits but including FCS octets).
Jabbers	The number of packets received during this interval that were longer than 1518 octets (excluding framing bits but including FCS octets) and were not an integral number of octets in length or had a bad FCS.

Hosts Control Table

The following fields appear in the Hosts Control Table.

Field	Description
Data Source	The source of the data for this instance of the host function. The source can be any interface on the device.
Size	The number of host entries in the table.
Last Deleted	The value of sysUpTime when the last entry was deleted from the portion of the table associated with this entry.
Owner	The entity that configured this entry and is using the resources assigned to it.
Status	The status of this host entry.

Host Table

The following fields appear in the Host Table.

Field	Description
Index	The set of collected host statistics of which this entry is a part.
Address	The physical address of this host.
Order	An index that defines the relative ordering of the creation time of hosts captured for a particular hostControlEntry.
In Packets	The number of packets without errors transmitted to this host since it was added to the Host Table.
Out Packets	The number of packets including errors transmitted by this address since it was added to the Host Table.
In Octets	The number of octets transmitted to this address since it was added to the Host Table (excluding framing bits but including FCS octets) except for those octets in packets that contained errors.
Out Octets	The number of octets transmitted by this address since it was added to the Host Table (excluding framing bits but including FCS octets) including those octets in packets that contained errors.
Out Errors	The number of error packets transmitted by this address since it was added to the Host Table.
Out Multicast	The number of good packets transmitted by this address that were directed to a multicast address since it was added to the Host Table. This value does not include packets directed to the broadcast address.
Out Broadcast	The number of good packets transmitted by this address that were directed to the broadcast address since it was added to the Host Table.

Host Table Detail

The following fields appear in the Host Table Detail view.

Field	Description
MAC Address	The physical address of this device.
Out Octets	The number of octets transmitted by this address since it was added to the Host Table (excluding framing bits but including FCS octets) including those octets in packets that contained errors.
In Octets	The number of octets transmitted to this address since it was added to the Host Table (excluding framing bits but including FCS octets) except for those octets in packets that contained errors.
Out Packets	The number of packets including errors transmitted by this address since it was added to the Host Table.
In Packets	The number of packets without errors transmitted to this host since it was added to the Host Table.
Errors	The number of error packets transmitted by this address since it was added to the Host Table.
Broadcast	The number of good packets transmitted by this address that were directed to the broadcast address since it was added to the Host Table.
Multicast	The number of good packets transmitted by this address that were directed to a multicast address since it was added to the Host Table. This value does not include packets directed to the broadcast address.

Matrix Control Table

The following fields appear in the Matrix Control Table.

Field	Description
Data Source	The source of the data from which this entry creates a traffic matrix. The source can be any interface on the device.
Size	The number of matrix entries in the table for this interface.
Last Deleted	The value of sysUpTime when the last entry was deleted from the portion of the matrixSDTable or matrixDSTable associated with this entry.
Owner	The entity that configured this entry and is using the resources assigned to it.
Status	The status of this entry.

Matrix Table

The following fields appear in the Matrix Table.

Field	Description
Source	The source physical address.
Destination	The destination physical address.
Packets	The number of packets transmitted from the source address to the destination address (includes error packets).
Octets	The number of octets (excluding framing bits but including FCS octets) contained in all packets transmitted from the source address to the destination address.
Errors	The number of error packets transmitted from the source address to the destination address.

HostTopN Control Table

The following fields appear in the HostTopN Control Table.

Field	Description
Data Source	The source of the data. This source can be any interface on the device.
Report	The HostTopN Control Table report of which this entry is a part.
ReqSize	The maximum number of hosts requested for the HostTopN Control Table.
Size	The maximum number of hosts in the table.
Duration	The number of seconds that this report has collected during the last sampling interval or, if this report is currently being collected, the number of seconds that this report is being collected during this sampling interval.
Started	The value of sysUpTime when this report was last started.
Time Left	The number of seconds left in the report currently being collected.
Owner	The entity that configured this entry and is therefore using the resources assigned to it.

Top Hosts View

The following fields appear in the Top Hosts view.

Field	Description
Top Hosts	The maximum number of hosts requested for the table. The default is 10.
Sample Interval	The number of seconds that this report has collected during the last sampling interval or, if this report is currently being collected, the number of seconds that this report is being collected during this sampling interval.
Time Left in Sample	The number of seconds left in the report currently being collected.
Report Type	This object identifies the TopN report of which this entry is a part.
Data Source	The source of the data. This source can be any interface on the device.
Index	An index that uniquely identifies an entry in the table among those in the same report.
Address	The physical address of this host.
Rate Value	The amount of change in the selected variable during this sampling interval.

Appendix B

Token Ring Fields and Statistics

This appendix describes the Token Ring fields and statistics that appear in the RMON Management Module. The fields and statistics are listed according to the RMON table or view on which they are found.

Mac-Layer Statistics Table

This table provides a list of Mac-Layer Token Ring statistic entries.

Field	Description
Data Source	The source of the data that this entry is configured to analyze. The source can be any Token Ring interface on this device.
Octets	The total number of octets of data in MAC packets (excluding those that were not good frames) received on the network (excluding framing bits but including FCS octets.
Packets	The total number of MAC packets (excluding packets that were not good frames) received.
BeaconPkts	The total number of beacon MAC packets detected by the probe.
ClaimPkts	The total number of claim token MAC packets detected by the probe.
PurgePkts	The total number of ring purge MAC packets detected by the probe.
Owner	The entity that configured this entry and is using the resources assigned to it.

Mac-Layer Statistics Detail View

The following fields appear on the Mac-Layer Statistics detail view.

Isolating Errors Chart

The following fields appear in the Isolating Errors Chart.

Field	Description
Line	The total number of line errors reported in error reporting packets detected by the probe.
Burst	The total number of burst errors reported in error reporting packets detected by the probe.
A/C	The total number of AC (address copied) errors reported in error reporting packets detected by the probe.
Abort	The total number of abort delimiters reported in error reporting packets detected by the probe.
Internal	The total number of adapter internal errors reported in error reporting packets detected by the probe.
Total	The total number of errors reported.

Non-Isolating Errors Chart

The following fields appear in the Non-Isolating Errors Chart.

Field	Description
Lost Frames	The total number of lost frame errors reported in error reporting packets detected by the probe.
Congestion	The total number of receive congestion errors reported in error reporting packets detected by the probe.
Frame Copied	The total number of frame copied errors reported in error reporting packets detected by the probe.
Token	The total number of token errors reported in error reporting packets detected by the probe.

Field	Description
Frequency	The total number of frequency errors reported in error reporting packets detected by the probe.
Total	The total number of errors reported.

Event Breakdown Chart

The following fields appear in the Event Breakdown Chart.

Field	Description
Drop Events	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is the number of times this condition has been detected.
Claim Token	The total number of times that the ring enters the claim token state from normal ring state or ring purge state.
Ring Purge	The total number of times the ring enters the ring purge state from normal ring state.
Ring Poll	The total number of ring poll events detected by the probe (i.e., the number of ring polls initiated by the active monitor that were detected).
Beacon	The total number of times the ring enters a beaconing state from a non-beaconing state.
Total	The total number of events reported.

Mac-Layer History Control Table

The following fields appear on the Mac-Layer History Control Table.

Field	Description
Data Source	The source of the data for which historical data was collected and placed in a media-specific table on behalf of this entry. The source can be any interface on the device.
Interval	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this history control entry.
SizeReq	The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.
Size	The number of discrete sampling intervals over which data has been saved in the part of the media-specific table associated with this entry.
Owner	The entity that configured this entry and is using the resources assigned to it.
Status	The Status of this entry.

Mac-Layer History Table

The following fields and statistics appear in the Mac-Layer History Table.

Field	Description
Created	The value of sysUpTime at the start of the interval over which this sample was measured. If the probe keeps track of the time of day, it starts the first sample when the next hour of the day begins.
Stations	The maximum number of active stations on the ring detected by the probe during this sampling interval.
Octets	The total number of octets of data in MAC packets (excluding those that were not good frames) received on the network during this sampling interval (excluding framing bits but including FCS octets).
Packets	The total number of MAC packets (excluding those there were not good frames) received during this sampling interval.

Field	Description
PrgePkts	The total number of ring purge MAC packets detected by the probe during this sampling interval.
ClmTkPkts	The total number of claim token MAC packets detected by the probe during this sampling interval.
BecnPckts	The total number of beacon MAC packets detected by the probe during this sampling interval.
BecnTime	The amount of time that the ring has been in the beaconing state during this sampling interval.
NAUNChng	The total number of NAUN changes detected by the probe during this sampling interval.
AbortErrs	The total number of abort delimiters reported in error reporting packets detected by the probe during this sampling interval.
ACErrs	The total number of AC (address copied) errors reported in error reporting packets detected by the probe during this sampling interval.
BrstErrs	The total number of burst errors reported in error reporting packets detected by the probe during this sampling interval.
CngstErrs	The total number of receive congestion errors reported in error reporting packets detected by the probe during this sampling interval.
FrCpyErrs	The total number of frame copied errors reported in error reporting packets detected by the probe during this sampling interval.
FreqErrs	The total number of frequency errors reported in error reporting packets detected by the probe during this sampling interval.
IntrnErrs	The total number of adapter internal errors reported in error reporting packets detected by the probe during this sampling interval.
LineErrs	The total number of line errors reported in error reporting packets detected by the probe during this sampling interval.
LstFrErrs	The total number of lost frame errors reported in error reporting packets detected by the probe during this sampling interval.
TokenErrs	The total number of token errors reported in error reporting packets detected by the probe during this sampling interval.
SftErrRpt	The total number of soft error report frames detected by the probe during this sampling interval.
RgPolEvnts	The total number of ring poll events detected by the probe during this sampling interval.

Field	Description
PurgeEvnts	The total number of times that the ring entered the ring purge state from normal ring state during this sampling interval.
DropEvnts	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval.
ClmTkEvnts	The total number of times that the ring enters the claim token state from normal ring state or ring purge state during this sampling interval.
BecnEvnts	The total number of times that the ring enters a beaconing state during this sampling interval.

Promiscuous Statistics Table

This table provides a list of Promiscuous Token Ring Statistic entries.

Field	Description
Data Source	The source of the data that this entry is configured to analyze. The source can be any Token Ring interface on this device.
Octets	The total number of octets of data in good frames received on the network (excluding framing bits, but including FCS octets) in non-MAC packets.
Packets	The total number of non-MAC packets (excluding packets that were not good frames) received.
Broadcasts	The total number of good non-MAC frames received that were directed to an LCC braodcast address (0XFFFFFFFFFFFF) or (0XC000FFFFFFFF)
Multicasts	The total number of good non-MAC frames directed to a local or global multicast or functional address (not including broadcast address).
Drop Events	The total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is the number of times this condition has been detected.
Owner	The entity that configured this entry and is using the resources assigned to it.

Promiscuous Statistics Detail View

The following fields appear on the Promiscuous Statistics detail view.

Frame Size Breakdown

The following fields appear in the Frame Size Breakdown Chart.

Field	Description
18-63	The total number of good Non-MAC frames received that were between 18 and 63 octets in length inclusive, excluding framing bits but including FCS octets.
64-127	The total number of good Non-MAC frames received that were between 64 and 127 octets in length inclusive, excluding framing bits but including FCS octets.
128-255	The total number of good Non-MAC frames received that were between 128 and 255 octets in length inclusive, excluding framing bits but including FCS octets.
256-511	The total number of good Non-MAC frames received that were between 256 and 511 octets in length inclusive, excluding framing bits but including FCS octets.
512-1023	The total number of good Non-MAC frames received that were between 512 and 1023 octets in length inclusive, excluding framing bits but including FCS octets.
1024-2047	The total number of good Non-MAC frames received that were between 1024 and 2047 octets in length inclusive, excluding framing bits but including FCS octets.
2048-4095	The total number of good Non-MAC frames received that were between 2048 and 4095 octets in length inclusive, excluding framing bits but including FCS octets.
4096-8191	The total number of good Non-MAC frames received that were between 4096 and 8191 octets in length inclusive, excluding framing bits but including FCS octets.
8192-18,000	The total number of good Non-MAC frames received that were between 8192 and 18,000 octets in length inclusive, excluding framing bits but including FCS octets.
greater than 18,000	The total number of good Non-MAC frames received that were greater than 18,000 octets in length inclusive, excluding framing bits but including FCS octets.

Promiscuous History Control Table

The following fields appear on the Promiscuous History Control Table.

Field	Description
Data Source	The source of the data for which historical data was collected and placed in a media-specific table on behalf of this entry. The source can be any interface on the device.
Interval	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this history control entry.
SizeReq	The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.
Size	The number of discrete sampling intervals over which data has been saved in the part of the media-specific table associated with this entry.
Owner	The entity that configured this entry and is using the resources assigned to it.
Status	The Status of this entry.

Promiscuous History Table

The following fields and statistics appear in the Promiscuous History Table.

Field	Description
Created	The value of sysUpTime at the start of the interval over which this sample was measured. If the probe keeps track of the time of day, it starts the first sample when the next hour of the day begins.
Octets	The total number of octets of data in non-MAC packets (excluding those that were not good frames) received on the network during this sampling interval (excluding framing bits but including FCS octets).
Packets	The total number of non-MAC packets (excluding those there were not good frames) received during this sampling interval.

Field	Description
Broadcasts	The total number of good non-MAC frames received that were directed to an LCC braodcast address (0XFFFFFFFFFFFF) or (0XC000FFFFFFFF)
Multicasts	The total number of good non-MAC frames directed to a local or global multicast or functional address (not including broadcast address).
Drop Events	The total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is the number of times this condition has been detected.
18-63	The total number of good Non-MAC frames received that were between 18 and 63 octets in length inclusive, excluding framing bits but including FCS octets.
64-127	The total number of good Non-MAC frames received that were between 64 and 127 octets in length inclusive, excluding framing bits but including FCS octets.
128-255	The total number of good Non-MAC frames received that were between 128 and 255 octets in length inclusive, excluding framing bits but including FCS octets.
256-511	The total number of good Non-MAC frames received that were between 256 and 511 octets in length inclusive, excluding framing bits but including FCS octets.
512-1023	The total number of good Non-MAC frames received that were between 512 and 1023 octets in length inclusive, excluding framing bits but including FCS octets.
1024-2047	The total number of good Non-MAC frames received that were between 1024 and 2047 octets in length inclusive, excluding framing bits but including FCS octets.
2048-4095	The total number of good Non-MAC frames received that were between 2048 and 4095 octets in length inclusive, excluding framing bits but including FCS octets.
4096-8191	The total number of good Non-MAC frames received that were between 4096 and 8191 octets in length inclusive, excluding framing bits but including FCS octets.
8192-18,000	The total number of good Non-MAC frames received that were between 8192 and 18,000 octets in length inclusive, excluding framing bits but including FCS octets.
greater than 18,000	The total number of good Non-MAC frames received that were greater than 18,000 octets in length inclusive, excluding framing bits but including FCS octets.

Hosts Tables

Refer to Appendix A for a description of the fields that appear in the Hosts Control Table, the Host Table, and the Host Table Detail.

Matrix Tables

Refer to Appendix A for a description of the fields that appear in the Matrix Control Table and the Matrix Table.

HostTopN Tables

Refer to Appendix A for a description of the fields that appear in the HostTopN Control Table and the Top Hosts View.

Ring Station Control View

The following fields and statistics appear in the Ring Station Control table.

Field	Description
Interface	A value that uniquely identifies the interface on this remote network monitoring device from which data is collected.
Ring State	The current status of this ring.
Active Monitor	The address of the active monitor on this segment.
Table Size	The number of Ring Station entries in the Ring Station Table associated with this entry.
Active Stations	The number of active Ring Station entries in the Ring Station Table associated with this entry.
Order Changes	The number of add and delete events in the Ring Station Control Table optionally associated with this entry.
Beacon Sender	The address of the sender of the last beacon frame received by the probe on this ring.
Beacon NAUN	The address of the NAUN in the last beacon frame received by the probe on this ring.
Address	The physical address of this station.

Field	Description
Last NAUN	The physical address of the last known NAUN of this station.
Last Entered	The value of sysUpTime at the time this station last entered the ring.
Last Exited	The value of sysUpTime at the time the probe detected that this station last exited the ring.
Status	The status of this station on the ring.

Station Order Table

The following fields appear on the Station Order Table.

Field	Description
Order	The location of this station with respect to other stations on the ring when the RMON probe gets the value one.
Address	The physical address of this station.

Non-Isolating Errors

The following fields appear when you click on the Non-Isolating Errors button:

Field	Description
Address	The physical address of the station.
Token	The total number of token errors reported by the station in error reporting frames detected by the probe.
Duplicates	The number of times the station experienced a duplicate address error.
Lost Frame	The total number of lost frame errors reported by this station in error reporting packets detected by the probe.

Field	Description
Copy Frame	The total number of frame copied errors reported by this station in error reporting packets detected by the probe.
Frequency	The total number of frequency errors reported by this station in error reporting packets detected by the probe.
Insertion	The number of times the probe detected this station inserting onto the ring.
In Beacon	The total number of beacon frames sent by this station and detected by the probe.
Out Beacon	The total number of beacon frames detected by the probe that name this station as the NAUN.

Isolating Errors

The following fields appear when you click on the Isolating Errors button.

Field	Description
Address	The physical address of this station.
In Line	The total number of line errors reported by this station in error reporting packets detected by the probe.
Out Line	The total number of line errors reported in error reporting packets sent by the nearest active downstream neighbor of this station and detected by the probe.
In Burst	The total number of burst errors reported by this station in error reporting packets detected by the probe.
Out Burst	The total number of burst errors reported in error reporting packets sent by the nearest active downstream neighbor of this station and detected by the probe.
A/C	The total number of AC (address copied) errors reported in error reporting packets sent by the nearest active downstream neighbor of this station and detected by the probe.
Abort	The total number of abort delimiters reported by this station in error reporting packets detected by the probe.

Field	Description
Internal	The total number of adapter internal errors reported by this station in error reporting packets detected by the probe.
Congestion	The total number of receive congestion errors reported by this station in error reporting packets detected by the probe.

Appendix C

SpectroWATCH

This appendix contains information on using SpectroWATCH with the RMON Management Module.

Watches

The RMON Management Module uses SpectroWATCH to perform various calculations on the parameters of the RMON Statistics Groups. These calculations are specified as Watches for the RMONEthProbe and RMONTRProbe model types.

The calculations provide aggregate information such as segment performance information as well as individual rate calculations for each Statistic Group parameter. This data may be utilized in a variety of ways, such as in a user created GIB used to dynamically monitor these values, or by making these Watches logged and writing the results to Spectrum's archive system. When the results are written to Spectrum's archive system, the system enables historical reporting on the data using Spectrum Reports. These calculations are also the source for Monitor Point performance statistics rolled up to a Network model when a Probe model is used as the Network's Monitor Point.

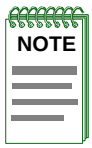
Enabling Rmon Watches

A complete set of Watches for Statistic Group parameters is provided with the RMON Management Module for both the RMONEthProbe and RMONTRProbe model types. These are listed in the following section.

The watches are fully configured and set to active by default. Therefore, the user is not required to start or work with SpectroWATCH to get started.

However, this feature is enabled for RMON model types only when the Probe has been copied into a Network model as a Monitor Point candidate. Attempting to utilize these Watch attributes otherwise will result in a failure.

For information on how to make a Probe model a Monitor Point, and thus enable its RMON Watches, see section 2.4, Configuring RMON as a Network Monitor Point.



In the following sections, for information on how to Create, Modify or Log a Watch, please refer to the SpectroWATCH Users Guide.

Modifying or Creating Watches

A user may modify any of the supplied watches or create new ones. It is recommended that no changes be made to the following Watches, as these are used by Spectrum's Monitor Point Performance Views and changes will result in inconsistencies between these Views and the RMON Segment Performance Views of the Probes.

RMONEProbe
MonUtilization
MonBitsUsedPerSec
MonErrorRate
MonPacketRate
MonCollisionRate

RMONTProbe
TR_Mon_Util
TR_Mon_Frame_Rate
TR_Mon_Errs_Per_MFrame
TR_Mon_Active_Staions

Using Rmon Watches

A complete set of Watches for the RMON Statistics Groups has been provided for general purpose use and may be modified by the user without affecting other Spectrum functions.

These Watches are identified by names beginning with mp_Mon. For example,

RMONEthProbe
mp_MonPackets
mp_MonOctets

RMONTRProbe
mp_MonMLPackets
mp_MonMLOctets

Logging Watches

The user may enable logging on any of the Watch attributes as detailed in the SpectroWATCH Users Guide.

Ethernet Watches

The following Watches are provided for the RMONEthProbe model type:

```
MonUtilization=            ((MonBitsUsedPerSec*100)/MonBandwidth)
-------------------------------------------------------------------

MonBitsUsedPerSec=         INTEGER((((COUNTER_DELTA
                           (mp_ethStsOctets)*8)+
                           (COUNTER_DELTA(mp_ethStsPkts)*160))/
                           COUNTER_DELTA(TIME)))
-------------------------------------------------------------------

MonPacketRate=             INTEGER((MonDeltaTotalPackets/
                           COUNTER_DELTA(TIME)))
-------------------------------------------------------------------

MonDeltaTotalPackets=      COUNTER_DELTA(mp_ethStsPkts)
-------------------------------------------------------------------

MonHardErrorRate=          INTEGER(((MonHardErrorCount*100)/
                           MonDeltaTotalPackets))
-------------------------------------------------------------------

MonErrorRate=              MonHardErrorRate
-------------------------------------------------------------------

MonHardErrorCount=         INTEGER(((((COUNTER_DELTA
                           (mp_ethStsCRCAlgnErr)
                           +COUNTER_DELTA(mp_ethStsOverPkts))
                           +COUNTER_DELTA(mp_ethStsUnderPkts))
                           +COUNTER_DELTA(mp_ethStsFragments))
                           +COUNTER_DELTA(mp_ethStsJabbers)))
-------------------------------------------------------------------

MonCollisionRate=   INTEGER(((COUNTER_DELTA(mp_ethStsCollision)
                    *100)/MonDeltaTotalPackets ))
-------------------------------------------------------------------

MonSystemUptime=           Mem_Sys_Up_Time
-------------------------------------------------------------------

mp_MonOctets=              INTEGER((COUNTER_DELTA(
                           mp_ethStsOctets)/COUNTER_DELTA( TIME)))
-------------------------------------------------------------------

mp_MonPackets=             INTEGER((COUNTER_DELTA( mp_ethStsPkts)/
                           COUNTER_DELTA(TIME)))
-------------------------------------------------------------------
```

```
mp_MonBroadPkts=          INTEGER(((COUNTER_DELTA
                          (mp_ethStsBroadPkts) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonMultiPkts=          INTEGER(((COUNTER_DELTA
                          (mp_ethStsMultiPkts) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonCRCAlgnErrs=        INTEGER(((COUNTER_DELTA
                          (mp_ethStsCRCAlgnErr) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonUnderPkts=          INTEGER(((COUNTER_DELTA
                          (mp_ethStsUnderPkts) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonOverPkts=           INTEGER(((COUNTER_DELTA
                          (mp_ethStsOverPkts)*100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonFragments=          INTEGER(((COUNTER_DELTA
                          (mp_ethStsFragments) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonJabbers=            INTEGER(((COUNTER_DELTA
                          (mp_ethStsJabbers)*100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonCollisions=         INTEGER(((COUNTER_DELTA
                          (mp_ethStsCollision) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonPkts64=             INTEGER(((COUNTER_DELTA
                          (mp_ethStsPkts64)*100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonPkts65to127=        INTEGER(((COUNTER_DELTA
                          (mp_ethStsPkts65to127) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonPkts128to255=       INTEGER(((COUNTER_DELTA
                          (mp_ethStsPkts128to255) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonPkts256to511=       INTEGER(((COUNTER_DELTA
                          (mp_ethStsPkts256to511) *100)/
                          COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------
```

```
mp_MonPkts512to1023=       INTEGER(((COUNTER_DELTA
                           (mp_ethStsPkts512to1023) *100)/
                           COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------

mp_MonPkts1024to1518=      INTEGER(((COUNTER_DELTA
                           (mp_ethStsPkts1024to 1518)*100)
                           COUNTER_DELTA(mp_ethStsPkts)))
-----------------------------------------------------------------
```

Token Ring Watches

The following watches are provided for the RMONTRProbe model type:

```
MonSystemUptime=           Mem_Sys_Up_Time
-----------------------------------------------------------------

MonBitsUsedPerSec=         (TR_Mon_Bytes_Per_Second*8)
-----------------------------------------------------------------

MonErrorRate=              TR_Mon_Errs_Per_MFrame
-----------------------------------------------------------------

MonBandwidth=              TR_Mon_Ring_Speed
-----------------------------------------------------------------

MonDeltaTotalPackets=      (COUNTER_DELTA(mp_mlayStsPkts)
                           +COUNTER_DELTA (mp_pStsPackets))
-----------------------------------------------------------------

MonHardErrorCount=         (TR_Mon_Isol_Err_Count+
                           TR_Mon_Non_Isol_Err_Count)
-----------------------------------------------------------------

MonHardErrorRate=          INTEGER(((MonHardErrorCount*100)/
                           MonDeltaTotalPackets ))
-----------------------------------------------------------------

MonPacketRate=             TR_Mon_Frame_Rate
-----------------------------------------------------------------

TR_Mon_Errs_Per_MFrame=    INTEGER((((TR_Mon_Isol_Err_Count+
                           TR_Mon_Non_Isol_Err_Count)*100)/
                           MonDeltaTotalPackets))
-----------------------------------------------------------------

TR_Mon_Bytes_Per_Second=   INTEGER(((COUNTER_DELTA
                           (mp_mlayStsOctets)
                           +COUNTER_DELTA(mp_pStsOctets))/
                           COUNTER_DELTA(TIME)))
-----------------------------------------------------------------
```

```
TR_Mon_Isol_Err_Count=     INTEGER (((((COUNTER_DELTA
                           (mp_mlayStsLineErrs)
                           +COUNTER_DELTA(mp_mlayStsInternErrs))
                           +COUNTER_DELTA(mp_mlayStsBurstErrs))
                           +COUNTER_DELTA(mp_mlayStsAbortErrs))
                           +COUNTER_DELTA(mp_mlayStsACErrs)))
-----------------------------------------------------------------

TR_Mon_Non_Isol_Err_Count= INTEGER(((((COUNTER_DELTA
                           (mp_mlayStsFrmCpyErrs)
                           +COUNTER_DELTA(mp_mlayStsLstFrmErrs))
                           +COUNTER_DELTA(mp_mlayStsTokenErrs))
                           +COUNTER_DELTA(mp_mlayStsFreqErrs))
                           +COUNTER_DELTA(mp_mlayStsCngstErrs)))
-----------------------------------------------------------------

TR_Mon_Frame_Rate=         INTEGER((MonDeltaTotalPackets/
                           COUNTER_DELTA(TIME)))
-----------------------------------------------------------------

TR_Mon_Ring_Speed=         mp_ifspeed
-----------------------------------------------------------------

TR_Mon_Active_Stations=    mp_activestations
-----------------------------------------------------------------

TR_Mon_Util=               (TR_Mon_Bytes_Per_Second/
                           TR_Mon_Ring_Speed )
-----------------------------------------------------------------
```

Appendix D

Sample Profiles

This appendix provides samples of properly formatted profiles for Ethernet and Token Ring.

Ethernet Profile

The following example shows an Ethernet profile for an agent or a device (such as an EMME) that has 4 network interfaces.

```
[OwnerString]
csi-defaults

[EnetStats]
1
2
3
4

[History]
1, 120, 30
2, 120, 30

[Host]
1
2
3

[Matrix}
1
2
3

[HostTopN]
1, 10, 3600
2, 25, 30
END.
```

Ethernet Profile Field Descriptions

In this enhanced version of Sample A, descriptions have been added for all fields in the profile.

[OwnerString]	Field identifier for the owner string specifier which follows. This must appear exactly as shown.
csi-defaults	The owner string. Assign a meaningful name, without spaces.
[EnetStats]	Field identifier for the Statistics Group specifiers which follow. This must appear exactly as shown. An instance of the Statistics Group may be configured for each network interface monitored by the RMON agent.
1 2 3 4	Statistics Group specifiers. This example creates an instance of Statistics for all 4 network interfaces of the EMME.
[History]	Field identifier for the History Group specifiers which follow. This must appear exactly as shown. An instance of the History Group may be configured for each network interface monitored by the RMON agent.
1, 120, 30 2, 120, 30	History Group specifiers. This example creates an instance of History for network interfaces 1 and 2 of the EMME. Field 1: Network interface (for example, 1 and 2) Field 2: Number of buckets (for example, 120 readings) Field 3: Interval over which to make a reading, in seconds (such as 30 seconds)
[Host]	Field identifier for the Host Group specifiers which follow. This must appear exactly as shown. An instance of the Host Group may be configured for each network interface monitored by the RMON agent.

1 2 3	Host Group specifiers. This example creates an instance of Host for 3 of the network interfaces of the EMME.
[Matrix}	Field identifier for the Matrix Group specifiers which follow. This must appear exactly as shown. An instance of the Matrix Group may be configured for each network interface monitored by the RMON agent.
1 2 3	Matrix Group specifiers. This example creates an instance of Matrix for 3 of the network interfaces of the EMME.
[HostTopN]	Field identifier for the HostTopN Group specifiers which follow. This must appear exactly as shown. An instance of the Host TopN Group may be configured for each network interface monitored by the RMON agent.
1, 10, 3600 2, 25, 30	HostTopN Group specifiers. This example creates an instance of HostTopN for 2 of the network interfaces of the EMME. Field 1: Network interface (for example, 1 and 2) Field 2: N (for example, Top 10 and Top 25) Field 3: Interval over which to make a reading, in seconds (such as 3600 seconds [one hour] and 30 seconds. These intervals begin when the profile is loaded.)
END.	End of profile. This must appear exactly as shown.

Token Ring Profile

The following example shows a sample profile for Token Ring for an agent or a device (such as a TRMM) that has 4 network interfaces.

```
[OwnerString]
csi-defaults

[MacStats]
1
2
3
4

[ProStats]
1
2

[History]
1, 120, 30
2, 120, 30

[Host]
1
2
3

[Matrix]
1
2
3

[HostTopN]
1, 10, 3600
2, 25, 30

END.
```

Token Ring Field Descriptions

In this enhanced version of Sample B, descriptions have been added for all fields in the profile.

[OwnerString]	Field identifier for the owner string specifier which follows. This must appear exactly as shown.
csi-defaults	The owner string. Assign a meaningful name, without spaces.
[MacStats]	Field identifier for the Mac-Layer Statistics Group specifiers which follow. This must appear exactly as shown.
1 2 3 4	Mac-Layer Statistics Group specifiers. This example creates an instance of Mac-Layer Statistics for all 4 network interfaces of the TRMM.
[ProStats]	Field identifier for the Promiscuous Statistics Group specifiers which follow. This must appear exactly as shown. An instance of the Promiscuous Statistics Group may be configured for each network interface monitored by the RMON agent.
1 2	Promiscuous Statistics Group specifiers. This example creates an instance of Promiscuous Statistics for all 4 network interfaces of the TRMM.
[History]	Field identifier for the History Group specifiers which follow. This must appear exactly as shown. An instance of the History Group may be configured for each network interface monitored by the RMON agent.
1, 120, 30 2, 120, 30	History Group specifiers. This example creates an instance of History for network interfaces 1 and 2 of the TRMM. Field 1: Network interface (for example, 1 and 2) Field 2: Number of buckets (for example, 120 readings) Field 3: Interval over which to make a reading, in seconds (such as 30 seconds)

[Host]	Field identifier for the Host Group specifiers which follow. This must appear exactly as shown. An instance of the Host Group may be configured for each network interface monitored by the RMON agent.
1 2 3	Host Group specifiers. This example creates an instance of Host for 3 of the network interfaces of the TRMM.
[Matrix}	Field identifier for the Matrix Group specifiers which follow. This must appear exactly as shown. An instance of the Matrix Group may be configured for each network interface monitored by the RMON agent.
1 2 3	Matrix Group specifiers. This example creates an instance of Matrix for 3 of the network interfaces of the TRMM.
[HostTopN]	Field identifier for the HostTopN Group specifiers which follow. This must appear exactly as shown. An instance of the Host TopN Group may be configured for each network interface monitored by the RMON agent.
1, 10, 3600 2, 25, 30	HostTopN Group specifiers. This example creates an instance of HostTopN for 2 of the network interfaces of the TRMM. Field 1: Network interface (for example, 1 and 2) Field 2: N (for example, Top 10 and Top 25) Field 3: Interval over which to make a reading, in seconds (such as 3600 seconds [one hour] and 30 seconds. These intervals begin when the profile is loaded.)
END.	End of profile. This must appear exactly as shown.

Using a Wildcard to Specify All Network Interfaces

If you want to specify that all interfaces should be included in a sample, substitute an asterisk where you would normally specify the network interface, as shown in the following example.

```
[EnetStats]
*                   This example creates an instance of
                    Statistics for all network interfaces
                    monitored by the RMON agent.

[History]
*, 120, 30          This example creates 2 instances of History
                    for all
*, 120, 1800        network interfaces monitored by the RMON
                    agent.

                    Field 1: Network interface, (for example,
                    All)
                    Field 2: Number of buckets (for example, 120
                    readings)
                    Field 3: Interval over which to make a
                    reading, in seconds (for example, 30
                    seconds and 1800 seconds)
```

Appendix E

Object Identifiers (OIDs)

This chapter describes object identifiers (OIDs) of RMON objects that you can monitor, using the RMON Alarms feature. See *Configuring RMON Alarms and Events* for detailed information about using OIDs with alarms.

etherStats

OID	Object Name
1.3.6.1.2.1.16.1.1.1.1	etherStatsIndex
1.3.6.1.2.1.16.1.1.1.2	etherStatsDataSource
1.3.6.1.2.1.16.1.1.1.3	etherStatsDropEvents
1.3.6.1.2.1.16.1.1.1.4	etherStatsOctets
1.3.6.1.2.1.16.1.1.1.5	etherStatsPkts
1.3.6.1.2.1.16.1.1.1.6	etherStatsBroadcastPkts
1.3.6.1.2.1.16.1.1.1.7	etherStatsMulticastPkts
1.3.6.1.2.1.16.1.1.1.8	etherStatsCRCAlignErrors
1.3.6.1.2.1.16.1.1.1.9	etherStatsUndersizePkts
1.3.6.1.2.1.16.1.1.1.10	etherStatsOversizePkts
1.3.6.1.2.1.16.1.1.1.11	etherStatsFragments
1.3.6.1.2.1.16.1.1.1.12	etherStatsJabbers
1.3.6.1.2.1.16.1.1.1.13	etherStatsCollisions
1.3.6.1.2.1.16.1.1.1.14	etherStatsPkts64Octets
1.3.6.1.2.1.16.1.1.1.15	etherStatsPkts65to127Octets
1.3.6.1.2.1.16.1.1.1.16	etherStatsPkts128to255Octets
1.3.6.1.2.1.16.1.1.1.17	etherStatsPkts256to511Octets
1.3.6.1.2.1.16.1.1.1.18	etherStatsPkts512to1023Octets
1.3.6.1.2.1.16.1.1.1.19	etherStatsPkts1024to1518Octets
1.3.6.1.2.1.16.1.1.1.20	etherStatsOwner
1.3.6.1.2.1.16.1.1.1.21	etherStatsStatus

historyControl

OID	Object Name
1.3.6.1.2.1.16.2.1.1.1	historyControlIndex
1.3.6.1.2.1.16.2.1.1.2	historyControlDataSource
1.3.6.1.2.1.16.2.1.1.3	historyControlBucketsRequested
1.3.6.1.2.1.16.2.1.1.4	historyControlBucketsGranted
1.3.6.1.2.1.16.2.1.1.5	historyControlInterval
1.3.6.1.2.1.16.2.1.1.6	historyControlOwner
1.3.6.1.2.1.16.2.1.1.7	historyControlStatus

etherHistory

OID	Object Name
1.3.6.1.2.1.16.2.2.1.1	etherHistoryIndex
1.3.6.1.2.1.16.2.2.1.2	etherHistorySampleIndex
1.3.6.1.2.1.16.2.2.1.3	etherHistoryIntervalStart
1.3.6.1.2.1.16.2.2.1.4	etherHistoryDropEvents
1.3.6.1.2.1.16.2.2.1.5	etherHistoryOctets
1.3.6.1.2.1.16.2.2.1.6	etherHistoryPkts
1.3.6.1.2.1.16.2.2.1.7	etherHistoryBroadcastPkts
1.3.6.1.2.1.16.2.2.1.8	etherHistoryMulticastPkts
1.3.6.1.2.1.16.2.2.1.9	etherHistoryCRCAlignErrors
1.3.6.1.2.1.16.2.2.1.10	etherHistoryUndersizePkts
1.3.6.1.2.1.16.2.2.1.11	etherHistoryOversizePkts
1.3.6.1.2.1.16.2.2.1.12	etherHistoryFragments
1.3.6.1.2.1.16.2.2.1.13	etherHistoryJabbers
1.3.6.1.2.1.16.2.2.1.14	etherHistoryCollisions
1.3.6.1.2.1.16.2.2.1.15	etherHistoryUtilization

hostControl

OID	Object Name
1.3.6.1.2.1.16.4.1.1.1	hostControlIndex
1.3.6.1.2.1.16.4.1.1.2	hostControlDataSource
1.3.6.1.2.1.16.4.1.1.3	hostControlTableSize
1.3.6.1.2.1.16.4.1.1.4	hostControlLastDeleteTime
1.3.6.1.2.1.16.4.1.1.5	hostControlOwner

OID	Object Name
1.3.6.1.2.1.16.4.1.1.6	hostControlStatus

host

OID	Object Name
1.3.6.1.2.1.16.4.2.1.1	hostAddress
1.3.6.1.2.1.16.4.2.1.2	hostCreationOrder
1.3.6.1.2.1.16.4.2.1.3	hostIndex
1.3.6.1.2.1.16.4.2.1.4	hostInPkts
1.3.6.1.2.1.16.4.2.1.5	hostOutPkts
1.3.6.1.2.1.16.4.2.1.6	hostInOctets
1.3.6.1.2.1.16.4.2.1.7	hostOutOctets
1.3.6.1.2.1.16.4.2.1.8	hostOutErrors
1.3.6.1.2.1.16.4.2.1.9	hostOutBroadcastPkts
1.3.6.1.2.1.16.4.2.1.10	hostOutMulticastPkts

hostTime

OID	Object Name
1.3.6.1.2.1.16.4.3.1.1	hostTimeAddress
1.3.6.1.2.1.16.4.3.1.2	hostTimeCreationOrder
1.3.6.1.2.1.16.4.3.1.3	hostTimeIndex
1.3.6.1.2.1.16.4.3.1.4	hostTimeInPkts
1.3.6.1.2.1.16.4.3.1.5	hostTimeOutPkts
1.3.6.1.2.1.16.4.3.1.6	hostTimeInOctets
1.3.6.1.2.1.16.4.3.1.7	hostTimeOutOctets
1.3.6.1.2.1.16.4.3.1.8	hostTimeOutErrors
1.3.6.1.2.1.16.4.3.1.9	hostTimeOutBroadcastPkts
1.3.6.1.2.1.16.4.3.1.10	hostTimeOutMulticastPkts

matrixControl

OID	Object Name
1.3.6.1.2.1.16.6.1.1.1	matrixControlIndex
1.3.6.1.2.1.16.6.1.1.2	matrixControlDataSource
1.3.6.1.2.1.16.6.1.1.3	matrixControlTableSize
1.3.6.1.2.1.16.6.1.1.4	matrixControlLastDeleteTime
1.3.6.1.2.1.16.6.1.1.5	matrixControlOwner
1.3.6.1.2.1.16.6.1.1.6	matrixControlStatus

matrixSD

OID	Object Name
1.3.6.1.2.1.16.6.2.1.1	matrixSDSourceAddress
1.3.6.1.2.1.16.6.2.1.2	matrixSDDestAddress
1.3.6.1.2.1.16.6.2.1.3	matrixSDIndex
1.3.6.1.2.1.16.6.2.1.4	matrixSDPkts
1.3.6.1.2.1.16.6.2.1.5	matrixSDOctets
1.3.6.1.2.1.16.6.2.1.6	matrixSDErrors

matrixDS

OID	Object Name
1.3.6.1.2.1.16.6.3.1.1	matrixDSSourceAddress
1.3.6.1.2.1.16.6.3.1.2	matrixDSDestAddress
1.3.6.1.2.1.16.6.3.1.3	matrixDSIndex
1.3.6.1.2.1.16.6.3.1.4	matrixDSPkts
1.3.6.1.2.1.16.6.3.1.5	matrixDSOctets
1.3.6.1.2.1.16.6.3.1.6	matrixDSErrors

hostTopNControl

OID	Object Name
1.3.6.1.2.1.16..5.1.1.1	hostTopNControlIndex
1.3.6.1.2.1.16..5.1.1.2	hostTopNHostIndex
1.3.6.1.2.1.16..5.1.1.3	hostTopNRateBase
1.3.6.1.2.1.16..5.1.1.4	hostTopNTimeRemaining
1.3.6.1.2.1.16..5.1.1.5	hostTopNDuration
1.3.6.1.2.1.16..5.1.1.6	hostTopNRequestedSize
1.3.6.1.2.1.16..5.1.1.7	hostTopNGrantedSize
1.3.6.1.2.1.16..5.1.1.8	hostTopNStartTime
1.3.6.1.2.1.16..5.1.1.9	hostTopNOwner
1.3.6.1.2.1.16..5.1.1.10	hostTopNStatus

hostTopN

OID	Object Name
1.3.6.1.2.1.16.5.2.1.1	hostTopNReport
1.3.6.1.2.1.16.5.2.1.2	hostTopNIndex
1.3.6.1.2.1.16.5.2.1.3	hostTopNAddress
1.3.6.1.2.1.16.5.2.1.4	hostTopNRate

alarm

OID	Object Name
1.3.6.1.2.16.3.1.1.1	alarmIndex
1.3.6.1.2.16.3.1.1.2	alarmInterval
1.3.6.1.2.16.3.1.1.3	alarmVariable
1.3.6.1.2.16.3.1.1.4	alarmSampleType
1.3.6.1.2.16.3.1.1.5	alarmValue
1.3.6.1.2.16.3.1.1.6	alarmStartupAlarm
1.3.6.1.2.16.3.1.1.7	alarmRisingThreshold
1.3.6.1.2.16.3.1.1.8	alarmFallingThreshold
1.3.6.1.2.16.3.1.1.9	alarmRisingEventIndex
1.3.6.1.2.16.3.1.1.10	alarmFallingEventIndex
1.3.6.1.2.16.3.1.1.11	alarmOwner
1.3.6.1.2.16.3.1.1.12	alarmStatus

event

OID	Object Name
1.3.6.1.2.1.16.9.1.1.1	eventIndex
1.3.6.1.2.1.16.9.1.1.2	eventDescription
1.3.6.1.2.1.16.9.1.1.3	eventType
1.3.6.1.2.1.16.9.1.1.4	eventCommunity
1.3.6.1.2.1.16.9.1.1.5	eventLastTimeSent
1.3.6.1.2.1.16.9.1.1.6	eventOwner
1.3.6.1.2.1.16.9.1.1.7	eventStatus

log

OID	Object Name
1.3.6.1.2.1.16.9.2.1.1	logEventIndex
1.3.6.1.2.1.16.9.2.1.2	logIndex
1.3.6.1.2.1.16.9.2.1.3	logTime
1.3.6.1.2.1.16.9.2.1.4	logDescription

tokenRingMLStats

OID	Object Name
1.3.6.1.2.1.16.1.2.1.1	tokenRingMLStatsIndex
1.3.6.1.2.1.16.1.2.1.2	tokenRingMLStatsDataSource
1.3.6.1.2.1.16.1.2.1.3	tokenRingMLStatsDropEvents
1.3.6.1.2.1.16.1.2.1.4	tokenRingMLStatsMacOctets
1.3.6.1.2.1.16.1.2.1.5	tokenRingMLStatsMacPkts
1.3.6.1.2.1.16.1.2.1.6	tokenRingMLStatsRingPurgeEvents
1.3.6.1.2.1.16.1.2.1.7	tokenRingMLStatsRingPurgePkts
1.3.6.1.2.1.16.1.2.1.8	tokenRingMLStatsBeaconEvents
1.3.6.1.2.1.16.1.2.1.9	tokenRingMLStatsBeaconTime
1.3.6.1.2.1.16.1.2.1.10	tokenRingMLStatsBeaconPkts
1.3.6.1.2.1.16.1.2.1.11	tokenRingMLStatsClaimTokenEvents
1.3.6.1.2.1.16.1.2.1.12	tokenRingMLStatsClaimTokenPkts
1.3.6.1.2.1.16.1.2.1.13	tokenRingMLStatsNAUNChanges
1.3.6.1.2.1.16.1.2.1.14	tokenRingMLStatsLineErrors
1.3.6.1.2.1.16.1.2.1.15	tokenRingMLStatsInternalErrors
1.3.6.1.2.1.16.1.2.1.16	tokenRingMLStatsBurstErrors
1.3.6.1.2.1.16.1.2.1.17	tokenRingMLStatsACErrors
1.3.6.1.2.1.16.1.2.1.18	tokenRingMLStatsAbortErrors
1.3.6.1.2.1.16.1.2.1.19	tokenRingMLStatsLostFrameErrors
1.3.6.1.2.1.16.1.2.1.20	tokenRingMLStatsCongestionErrors
1.3.6.1.2.1.16.1.2.1.21	tokenRingMLStatsFrameCopiedErrors
1.3.6.1.2.1.16.1.2.1.22	tokenRingMLStatsFrequencyErrors
1.3.6.1.2.1.16.1.2.1.23	tokenRingMLStatsTokenErrors
1.3.6.1.2.1.16.1.2.1.24	tokenRingMLStatsSoftErrorReports
1.3.6.1.2.1.16.1.2.1.25	tokenRingMLStatsRingPollEvents
1.3.6.1.2.1.16.1.2.1.26	tokenRingMLStatsOwner
1.3.6.1.2.1.16.1.2.1.27	tokenRingMLStatsStatus

tokenRingPStats

OID	Object Name
1.3.6.1.2.1.16.1.3.1.1	tokenRingPStatsIndex
1.3.6.1.2.1.16.1.3.1.2	tokenRingPStatsDataSource
1.3.6.1.2.1.16.1.3.1.3	tokenRingPStatsDropEvents
1.3.6.1.2.1.16.1.3.1.4	tokenRingPStatsDataOctets
1.3.6.1.2.1.16.1.3.1.5	tokenRingPStatsDataPkts
1.3.6.1.2.1.16.1.3.1.6	tokenRingPStatsDataBroadcastPkts
1.3.6.1.2.1.16.1.3.1.7	tokenRingPStatsDataMulticastPkts
1.3.6.1.2.1.16.1.3.1.8	tokenRingPStatsDataPkts18to63Octets
1.3.6.1.2.1.16.1.3.1.9	tokenRingPStatsDataPkts64to127Octets
1.3.6.1.2.1.16.1.3.1.10	tokenRingPStatsDataPkts128to255Octets
1.3.6.1.2.1.16.1.3.1.11	tokenRingPStatsDataPkts256to511Octets
1.3.6.1.2.1.16.1.3.1.12	tokenRingPStatsDataPkts512to1023Octets
1.3.6.1.2.1.16.1.3.1.13	tokenRingPStatsDataPkts1024to2047Octets
1.3.6.1.2.1.16.1.3.1.14	tokenRingPStatsDataPkts2048to4095Octets
1.3.6.1.2.1.16.1.3.1.15	tokenRingPStatsDataPkts4096to8191Octets
1.3.6.1.2.1.16.1.3.1.16	tokenRingPStatsDataPkts8192to18000Octets
1.3.6.1.2.1.16.1.3.1.17	tokenRingPStatsDataPktsGreaterThan18000Octets
1.3.6.1.2.1.16.1.3.1.18	tokenRingPStatsOwner
1.3.6.1.2.1.16.1.3.1.19	tokenRingPStatsStatus

tokenRingMLHistory

OID	Object Name
1.3.6.1.2.1.16.2.3.1.1	tokenRingMLHistoryIndex
1.3.6.1.2.1.16.2.3.1.2	tokenRingMLHistorySampleIndex
1.3.6.1.2.1.16.2.3.1.3	tokenRingMLHistoryIntervalStart
1.3.6.1.2.1.16.2.3.1.4	tokenRingMLHistoryDropEvents
1.3.6.1.2.1.16.2.3.1.5	tokenRingMLHistoryMacOctets
1.3.6.1.2.1.16.2.3.1.6	tokenRingMLHistoryMacPkts
1.3.6.1.2.1.16.2.3.1.7	tokenRingMLHistoryRingPurgeEvents
1.3.6.1.2.1.16.2.3.1.8	tokenRingMLHistoryRingPurgePkts
1.3.6.1.2.1.16.2.3.1.9	tokenRingMLHistoryBeaconEvents
1.3.6.1.2.1.16.2.3.1.10	tokenRingMLHistoryBeaconTime
1.3.6.1.2.1.16.2.3.1.11	tokenRingMLHistoryBeaconPkts
1.3.6.1.2.1.16.2.3.1.12	tokenRingMLHistoryClaimTokenEvents
1.3.6.1.2.1.16.2.3.1.13	tokenRingMLHistoryClaimTokenPkts
1.3.6.1.2.1.16.2.3.1.14	tokenRingMLHistoryNAUNChanges

OID	Object Name
1.3.6.1.2.1.16.2.3.1.15	tokenRingMLHistoryLineErrors
1.3.6.1.2.1.16.2.3.1.16	tokenRingMLHistoryInternalErrors
1.3.6.1.2.1.16.2.3.1.17	tokenRingMLHistoryBurstErrors
1.3.6.1.2.1.16.2.3.1.18	tokenRingMLHistoryACErrors
1.3.6.1.2.1.16.2.3.1.19	tokenRingMLHistoryAbortErrors
1.3.6.1.2.1.16.2.3.1.20	tokenRingMLHistoryLostFrameErrors
1.3.6.1.2.1.16.2.3.1.21	tokenRingMLHistoryCongestionErrors
1.3.6.1.2.1.16.2.3.1.22	tokenRingMLHistoryFrameCopiedErrors
1.3.6.1.2.1.16.2.3.1.23	tokenRingMLHistoryFrequencyErrors
1.3.6.1.2.1.16.2.3.1.24	tokenRingMLHistoryTokenErrors
1.3.6.1.2.1.16.2.3.1.25	tokenRingMLHistorySoftErrorReports
1.3.6.1.2.1.16.2.3.1.26	tokenRingMLHistoryRingPollEvents
1.3.6.1.2.1.16.2.3.1.27	tokenRingMLHistoryActiveStations

tokenRingPHistory

OID	Object Name
1.3.6.1.2.1.16.2.4.1.1	tokenRingPHistoryIndex
1.3.6.1.2.1.16.2.4.1.2	tokenRingPHistorySampleIndex
1.3.6.1.2.1.16.2.4.1.3	tokenRingPHistoryIntervalStart
1.3.6.1.2.1.16.2.4.1.4	tokenRingPHistoryDropEvents
1.3.6.1.2.1.16.2.4.1.5	tokenRingPHistoryDataOctets
1.3.6.1.2.1.16.2.4.1.6	tokenRingPHistoryDataPkts
1.3.6.1.2.1.16.2.4.1.7	tokenRingPHistoryDataBroadcastPkts
1.3.6.1.2.1.16.2.4.1.8	tokenRingPHistoryDataMulticastPkts
1.3.6.1.2.1.16.2.4.1.9	tokenRingPHistoryDataPkts18to63Octets
1.3.6.1.2.1.16.2.4.1.10	tokenRingPHistoryDataPkts64to127Octets
1.3.6.1.2.1.16.2.4.1.11	tokenRingPHistoryDataPkts128to255Octets
1.3.6.1.2.1.16.2.4.1.12	tokenRingPHistoryDataPkts256to511Octets
1.3.6.1.2.1.16.2.4.1.13	tokenRingPHistoryDataPkts512to1023Octets
1.3.6.1.2.1.16.2.4.1.14	tokenRingPHistoryDataPkts1024to2047Octets
1.3.6.1.2.1.16.2.4.1.15	tokenRingPHistoryDataPkts2048to4095Octets
1.3.6.1.2.1.16.2.4.1.16	tokenRingPHistoryDataPkts4096to8191Octets
1.3.6.1.2.1.16.2.4.1.17	tokenRingPHistoryDataPkts8192to18000Octets
1.3.6.1.2.1.16.2.4.1.18	tokenRingPHistoryDataPktsGreaterThan18000Octets

ringStationControl

OID	Object Name
1.3.6.1.2.1.16.10.1.1.1	ringStationControlIfIndex
1.3.6.1.2.1.16.10.1.1.2	ringStationControlTableSize
1.3.6.1.2.1.16.10.1.1.3	ringStationControlActiveStations
1.3.6.1.2.1.16.10.1.1.4	ringStationControlRingState
1.3.6.1.2.1.16.10.1.1.5	ringStationControlBeaconSender
1.3.6.1.2.1.16.10.1.1.6	ringStationControlBeaconNAUN
1.3.6.1.2.1.16.10.1.1.7	ringStationControlActiveMonitor
1.3.6.1.2.1.16.10.1.1.8	ringStationControlOrderChanges
1.3.6.1.2.1.16.10.1.1.9	ringStationControlStatus
1.3.6.1.2.1.16.10.1.1.10	ringStationControlOwner

ringStation

OID	Object Name
1.3.6.1.2.1.16.10.2.1.1	ringStationIfIndex
1.3.6.1.2.1.16.10.2.1.2	ringStationMacAddress
1.3.6.1.2.1.16.10.2.1.3	ringStationLastNAUN
1.3.6.1.2.1.16.10.2.1.4	ringStationStationStatus
1.3.6.1.2.1.16.10.2.1.5	ringStationLastEnterTime
1.3.6.1.2.1.16.10.2.1.6	ringStationLastExitTime
1.3.6.1.2.1.16.10.2.1.7	ringStationDuplicateAddresses
1.3.6.1.2.1.16.10.2.1.8	ringStationInLineErrors
1.3.6.1.2.1.16.10.2.1.9	ringStationOutLineErrors
1.3.6.1.2.1.16.10.2.1.10	ringStationInternalErrors
1.3.6.1.2.1.16.10.2.1.11	ringStationInBurstErrors
1.3.6.1.2.1.16.10.2.1.12	ringStationOutBurstErrors
1.3.6.1.2.1.16.10.2.1.13	ringStationACErrors
1.3.6.1.2.1.16.10.2.1.14	ringStationAbortErrors
1.3.6.1.2.1.16.10.2.1.15	ringStationLostFrameErrors
1.3.6.1.2.1.16.10.2.1.16	ringStationCongestionErrors
1.3.6.1.2.1.16.10.2.1.17	ringStationFrameCopiedErrors
1.3.6.1.2.1.16.10.2.1.18	ringStationFrequencyErrors
1.3.6.1.2.1.16.10.2.1.19	ringStationTokenErrors
1.3.6.1.2.1.16.10.2.1.20	ringStationInBeaconErrors
1.3.6.1.2.1.16.10.2.1.21	ringStationOutBeaconErrors
1.3.6.1.2.1.16.10.2.1.22	ringStationInsertions

ringStationOrder

OID	Object Name
1.3.6.1.2.1.16.10.3.1.1	ringStationOrderIfIndex
1.3.6.1.2.1.16.10.3.1.2	ringStationOrderOrderIndex
1.3.6.1.2.1.16.10.3.1.3	ringStationOrderMacAddress

ringStationConfigControl

OID	Object Name
1.3.6.1.2.1.16.10.4.1.1	ringStationConfigControlIfIndex
1.3.6.1.2.1.16.10.4.1.2	ringStationConfigControlMacAddress
1.3.6.1.2.1.16.10.4.1.3	ringStationConfigControlRemove
1.3.6.1.2.1.16.10.4.1.4	ringStationConfigControlUpdateStats

ringStationConfig

OID	Object Name
1.3.6.1.2.1.16.10.5.1.1	ringStationConfigIfIndex
1.3.6.1.2.1.16.10.5.1.2	ringStationConfigMacAddress
1.3.6.1.2.1.16.10.5.1.3	ringStationConfigUpdateTime
1.3.6.1.2.1.16.10.5.1.4	ringStationConfigLocation
1.3.6.1.2.1.16.10.5.1.5	ringStationConfigMicrocode
1.3.6.1.2.1.16.10.5.1.6	ringStationConfigGroupAddress
1.3.6.1.2.1.16.10.5.1.7	ringStationConfigFunctionalAddress

sourceRoutingStats

OID	Object Name
1.3.6.1.2.1.16.10.6.1.1	sourceRoutingStatsIfIndex
1.3.6.1.2.1.16.10.6.1.2	sourceRoutingStatsRingNumber
1.3.6.1.2.1.16.10.6.1.3	sourceRoutingStatsInFrames
1.3.6.1.2.1.16.10.6.1.4	sourceRoutingStatsOutFrames
1.3.6.1.2.1.16.10.6.1.5	sourceRoutingStatsThroughFrames
1.3.6.1.2.1.16.10.6.1.6	sourceRoutingStatsAllRoutesBroadcastFrames
1.3.6.1.2.1.16.10.6.1.7	sourceRoutingStatsSingleRouteBroadcastFrames
1.3.6.1.2.1.16.10.6.1.8	sourceRoutingStatsInOctets
1.3.6.1.2.1.16.10.6.1.9	sourceRoutingStatsOutOctets
1.3.6.1.2.1.16.10.6.1.10	sourceRoutingStatsThroughOctets
1.3.6.1.2.1.16.10.6.1.11	sourceRoutingStatsAllRoutesBroadcastOctets
1.3.6.1.2.1.16.10.6.1.12	sourceRoutingStatsSingleRoutesBroadcastOctets
1.3.6.1.2.1.16.10.6.1.13	sourceRoutingStatsLocalLLCFrames
1.3.6.1.2.1.16.10.6.1.14	sourceRoutingStats1HopFrames
1.3.6.1.2.1.16.10.6.1.15	sourceRoutingStats2HopsFrames
1.3.6.1.2.1.16.10.6.1.16	sourceRoutingStats3HopsFrames
1.3.6.1.2.1.16.10.6.1.17	sourceRoutingStats4HopsFrames
1.3.6.1.2.1.16.10.6.1.18	sourceRoutingStats5HopsFrames
1.3.6.1.2.1.16.10.6.1.19	sourceRoutingStats6HopsFrames
1.3.6.1.2.1.16.10.6.1.20	sourceRoutingStats7HopsFrames
1.3.6.1.2.1.16.10.6.1.21	sourceRoutingStats8HopsFrames
1.3.6.1.2.1.16.10.6.1.22	sourceRoutingStatsMoreThan8HopsFrames
1.3.6.1.2.1.16.10.6.1.23	sourceRoutingStatsOwner
1.3.6.1.2.1.16.10.6.1.24	sourceRoutingStatsStatus

Appendix F

Reports

This appendix describes the Report Information Block (.rib) files included with the RMON Management Module. The .rib files allow you to generate reports that display segment activity using RMON data from your probe device.

Report Description

RMON reports are run for a network segment using an RMON Probe model which is a Monitor Point for that segment. The data reported is RMON data from the Statistics Groups of your probe device.

Both aggregate performance data and individual parameter data are available.This data is collected and written to Spectrum's archival system by SpectroWATCH. Using SpectroWATCH allows the user to customize all data selection, calculations, logging intervals etc., including the addition of new Watches.

For more information on SpectroWATCH and the RMON Management Module, including the default SpectroWATCH Configuration for RMON, please refer to Appendix C, SpectroWATCH.

For more information on Spectrum Reports, see the **SPECTRUM Report Generator User's Guide**.

SetUp

Monitor Point

Only a Probe model which has been copied into the corresponding Network model as a Monitor Point can be used to run RMON Reports for that network segment. It is not necessary that the Probe model be selected as the current Monitor Point, only that it has been copied in as a candidate. For information on how to make a Probe model a Monitor Point, please refer to Section 2.4, Configuring RMON as a Network Monitor Point.

SpectroWATCH Logging

Once a Probe model is a Monitor Point, it is necessary to select which RMON data you want to make available for reports. This is accomplished with SpectroWATCH by enabling the logging option for the Watches you select .

See the following section describing the Cabletron supplied report generation (rib) files for a list of the RMON data available through these reports. If you wish to report on this data, it is necessary to select the logging option for each first. Note that making any other data logged will not be available until a rib file has been created which includes it.

For information on logging and SpectroWATCH, refer to the *SpectroWATCH Users's Guide*.

Statistical Reports

Report generation files are in the directory pointed to by the <CsRibpath>, which is designated in either the .Xdefaults or app-defaults/spectrum files. For more information on reports refer to the *SPECTRUM Report Generator's Guide.*

Standard Reports

Two report generation (rib) files are provided with the RMON management module, one for Ethernet and one for Token Ring. These report the segment performance data seen in the Spectrum Performance View of a Network model when the Probe model is the Monitor Point.

.../CsRib/RMONEthProbe/EProbePerf.rib

```
Performance View LabelAttributeAttributeID

LoadMonUtilization0x10207
Frame RateMonPacketRate0x10093
% ErrorsMonErrorRate0x10094
% CollisionsMonCollisionRate0x1024c
```

.../CsRib/RMONTRProbe/TProbePerf.rib

```
PerformanceView Label Attribute AttributeID

LoadTR_Mon_Util0x115ba
Frame RateTR_Mon_Frame_Rate0x115a7
Error RateTR_Mon_Errs_Per_MFrame0x115a8
StationsTR_Mon_Active_Stations0x118e2
```

Custom Reports

Additional RMON data is available for reporting. This data, detailed in Appendix C, SpectroWATCH, has been provided for each individual parameter of the RMON Statistics Groups. This enables the user to report on each statistic apart from an aggregate, and to provide a basis for custom performance calculations and reports.

These watches are identified by the name prefix 'mp_Mon'.

To utilize these watches, it is necessary to create custom rib files for this data. For information on creating rib files, refer to the *SPECTRUM Report Generator User's Guide.*

Running Reports

To generate a statistical report for a model, do the following;

1. Single click the probe model's icon to highlight it.
2. Select **Reports** from the file menu
3. Select **Generate** from the Reports menu.

4. Select **Statistical** as the Report type. The main window shows the selections for a Statistical Report. This information needs to be completed based on the *Report Generator User's Guide*.

5. Click **Generate**.

You will be prompted to specify report time frame parameters and a report output filename. When the report completes, it is placed in the SpectroGRAPH (SG) directory. The statistical report file is in the CsRib/<model type name> directory.

Sample Statistical Report Output File

The following is an example of tabular output from the default Ethernet Performance report.

```
RMONEProbe Performance Report Page: 1
Date: 04/02/96 16:04:44
Model Name: Enet Probe 1
Internet Addr:199.199.199.991
Device Type: RMONEthProbe
From Mon Apr 01 0:00:00 1996 To Mon Apr 01 23:59:59 1996

Poll TimeLoadFrame Rate%Errors%Collisions
04/01/96
09:04:02     4      298 0           0
09:05:023 267 0 0
09:06:024 281 0 0
09:07:022 280 0 0
09:08:025 340 0 0
09:09:024 361 0 0
09:10:02 5389 00
10:11:16 8 447 0 0
10:12:16 4 411 0 0
10:13:16 5 437 0 0
10:14:16 4 387 0 0
10:15:16 3 373 0 0
10:16:17 3 312 0 0
10:17:17 4 381 0 0
10:18:17 4 392 0 0
10:19:17 5 343 0 0
10:20:17 5 455 0 0
10:21:17 5 380 0 0
10:22:17 4 378 0 0

AVERAGES
   3.68 363.790.00 0.00
```

Index

Symbols

"Profile processing completed" 3-4, 3-6

Numerics

802.3 LAN segment 1-4

A

abort delimiters B-13
abort sequences 5-24, B-2
AC (Address Copied) errors B-13
active monitor B-11
active Ring Stations B-11
adapter internal errors B-5, B-14
Alarms 4-3
Alignment A-3

B

bad packets A-1
beacon MAC packets B-5
BrdcstPckts A-1
buffer overwrite prompt 7-3

C

claim token events B-6
claim token MAC packets B-5
Component Table 2-4
congestion errors 5-24, B-2
contact status values 7-5
Copy Frame B-13
CRC Errors A-5
Create Indirect Model button 7-2

D

Data Source
    Ethernet statistics A-1
    Hosts/Matrix Tables A-6, A-9
    Mac-Layer History Control Table B-4
delta performance status
    conditions 7-6
destination MAC addresses 1-5
Device Configuration View 2-4
Devices That Support RMON 1-6
distributing network monitoring
        functions 1-2
Drop Events A-5
duplicate address error B-12
Duplicates B-12

E

Error Detail View fields A-3
Ethernet History 4-3
Ethernet Statistics 4-3
extended monitoring capability 1-2

F

Frame Check Sequence A-2, A-3
frame copied errors 5-24, B-2
Frame Detail View fields A-2
frequency errors B-13

G

GnSNMPDev model type 2-2

H

History Table View A-4
History Table View fields A-4
Host Table Detail View
    fields A-8
Host Table View fields A-7, B-11
Hosts Control 4-3
HostTopN Control 4-3
    Table View fields A-9, B-11

I

In Octets A-7
In Packets A-7
Insertion B-13
interface B-11
internal errors 5-24, B-2

J

Jabbers A-4

L

line errors B-5
lost frame errors B-5
lost frames 5-24, B-2

M

Matrix Control 4-3
MltcstPkts A-1
Model Information 4-3
Model Type Name 2-2
Multicasts A-5

N

Navigate 4-3
Non-Isolating Station Errors View B-12
Non-Isolating Token Errors B-2
Notes 4-3
Notice i, iii

O

Off-Page Reference Icon
    Assembly 7-8
    button functions 7-8
Off-Page Reference Icon Assembly 7-8
out beacon frames B-13
Out Broadcast A-7
out burst errors B-13
out line errors B-13
Out Multicast A-7
Out Packets A-7
Oversized packets A-5

P

parsing mechanism 3-5
Poll Log Ratio 7-5
Polling (time) Interval 7-5
Profile Load/Unload
    error conditions 3-5

R

receive congestion errors B-14
Remote Network Monitoring 1-2
Reports F-1
ReqSize A-10
Restricted Rights Notice ii, iv
ring poll events B-3, B-5
ring purge MAC packets B-5
RMON Alarms/Events 4-3
RMONApp 1-4

S

security string 7-5
Select Model Type
    Dialog Box 7-2
soft error report frames B-5
SpectroWATCH C-1

T

Top Hosts Table View fields A-11, B-11
Trademarks i, iii
traffic-producing nodes 1-5

U

Undersized packets A-5
Unload Owner button 3-6
Utilities 4-3

V

Virus Disclaimer i, iv